VSG-1000

Vantage Service Gateway

User's Guide

Version 1.06

August 2004

Copyright

Copyright © 2004 by ZyXEL Communications Corporation.

Disclaimer

Trademarks

Interference Statements and Warnings

FCC Interference Statement

This device complies with Part 15 of the FCC rules. Operation is subject to the following two conditions:

(1) This device may not cause harmful interference.

(2) This device must accept any interference received, including interference that may cause undesired operations.

FCC Warning

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

CE Mark Warning:

This is a class A product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.

Taiwanese BSMI (Bureau of Standards, Metrology and Inspection) A Warning:

警告使用者
這是甲類的資訊產品，在居住的環境使用時，
可能造成射頻干擾，在這種情況下，
使用者會被要求採取某些適當的對策．

ZyXEL Limited Warranty

ZyXEL warrants to the original end user (purchaser) that this product is free from any defects in materials or workmanship for a period of up to two years from the date of purchase. During the warranty period, and upon proof of purchase, should the product have indications of failure due to faulty workmanship and/or materials, ZyXEL will, at its discretion, repair or replace the defective products or components without charge for either parts or labor, and to whatever extent it shall deem necessary to restore the product or components to proper operating condition. Any replacement will consist of a new or re-manufactured functionally equivalent product of equal value, and will be solely at the discretion of ZyXEL. This warranty shall not apply if the product is modified, misused, tampered with, damaged by an act of God, or subjected to abnormal working conditions.

Note

Repair or replacement, as provided under this warranty, is the exclusive remedy of the purchaser. This warranty is in lieu of all other warranties, express or implied, including any implied warranty of merchantability or fitness for a particular use or purpose. ZyXEL shall in no event be held liable for indirect or consequential damages of any kind of character to the purchaser.

To obtain the services of this warranty, contact ZyXEL's Service Center for your Return Material Authorization number (RMA). Products must be returned postage prepaid. It is recommended that the unit be insured when shipped.

Any returned products without proof of purchase or those with an out-dated warranty will be repaired or replaced (at the discretion of ZyXEL) and the customer will be billed for parts and labor. All repaired or replaced products will be shipped by ZyXEL to the corresponding return address, postage paid. This warranty gives you specific legal rights, and you may also have other rights that vary from country to country.

Online Registration

Don't forget to register your ZyXEL product (fast, easy online registration at www.zyxel.com) for free future product updates and information.

Customer Support

If you have questions about your ZyXEL product or desire assistance, contact ZyXEL Communications Corporation offices worldwide, in one of the following ways.

When you contact your customer support representative, have the following information ready:

♦ Warranty information.

♦ Date you received your product.

♦ Brief description of the problem and the steps you took to solve it.

METHOD / LOCATION	SUPPORT E-MAIL / SALES E-MAIL	TELEPHONE[1] / FAX[1]	WEB SITE / FTP SITE	REGULAR MAIL
WORLDWIDE	support@zyxel.com.tw / sales@zyxel.com.tw	+886-3-578-3942 / +886-3-578-2439	www.zyxel.com www.europe.zyxel.com ftp.zyxel.com ftp.europe.zyxel.com	ZyXEL Communications Corp. 6 Innovation Road II Science Park Hsinchu 300 Taiwan
NORTH AMERICA	support@zyxel.com / sales@zyxel.com	+1-800-255-4101 +1-714-632-0882 +1-714-632-0858	www.us.zyxel.com ftp.us.zyxel.com	ZyXEL Communications Inc. 1130 N. Miller St. Anaheim CA 92806-2001 U.S.A.
GERMANY	support@zyxel.de / sales@zyxel.de	+49-2405-6909-0 / +49-2405-6909-99	www.zyxel.de	ZyXEL Deutschland GmbH. Adenauerstr. 20/A2 D-52146 Wuerselen Germany
FRANCE	info@zyxel.fr	+33 (0)4 72 52 97 97 / +33 (0)4 72 52 19 20	www.zyxel.fr	ZyXEL France 1 rue des Vergers Bat. 1 / C 69760 Limonest France
SPAIN	support@zyxel.es / sales@zyxel.es	+34 902 195 420 / +34 913 005 345	www.zyxel.es	ZyXEL Communications Alejandro Villegas 33 1º, 28043 Madrid Spain
DENMARK	support@zyxel.dk / sales@zyxel.dk	+45 39 55 07 00 / +45 39 55 07 07	www.zyxel.dk	ZyXEL Communications A/S Columbusvej 5 2860 Soeborg Denmark
NORWAY	support@zyxel.no / sales@zyxel.no	+47 22 80 61 80 / +47 22 80 61 81	www.zyxel.no	ZyXEL Communications A/S Nils Hansens vei 13 0667 Oslo Norway
SWEDEN	support@zyxel.se / sales@zyxel.se	+46 31 744 7700 / +46 31 744 7701	www.zyxel.se	ZyXEL Communications A/S Sjöporten 4, 41764 Göteborg Sweden
FINLAND	support@zyxel.fi / sales@zyxel.fi	+358-9-4780-8411 / +358-9-4780 8448	www.zyxel.fi	ZyXEL Communications Oy Malminkaari 10 00700 Helsinki Finland

---

[1] "+" is the (prefix) number you enter to make an international telephone call.

Table of Contents

List of Figures

List of Tables

List of Diagrams

Preface

Congratulations on your purchase of the ZyXEL VSG-1000 Vantage Service Gateway.

The VSG-1000 Vantage Service Gateway is designed to provide Internet access to computers on a network with broadband service. Subscribers enjoy easy Internet connectivity with no extra configuration. In addition, you can set up basic billing functions and a subscriber database on the VSG-1000 to simplify management.

General Syntax Conventions

- "Enter" means for you to type one or more characters and press the carriage return. "Select" or "Choose" means for you to use one from the predefined choices.

- For brevity's sake, we will use "e.g." as shorthand for "for instance", and "i.e." as shorthand for "that is" or "in other words" throughout this manual.

- The "," notation indicates the sequence in which menus should be selected; for example "click **Window**, **Tile**" means you first click the **Windows** menu and then **Tile**.

- The ZyXEL VSG-1000 Vantage Service Gateway may be referred to as the VSG in this user's guide.

Related Documentation

ZyXEL Web Page and FTP Server Site

You can access release notes as well as system upgrades at ZyXEL web and FTP sites. Refer to the *Customer Support* page for more information.

User Guide Feedback

Help us help you. E-mail all User's Guide-related comments, questions or suggestions for improvement to techwriters@zyxel.com.tw or send regular mail to The Technical Writing Team, ZyXEL Communications Corp., 6 Innovation Road II, Science-Based Industrial Park, Hsinchu, 300, Taiwan. Thank you!

Part I:

Getting Started

This part introduces the VSG (Vantage Service Gateway), hardware installation, connections and basic system configuration using the web configurator.

Chapter 1
Getting to Know Your VSG

This chapter introduces the features and applications of the VSG.

1.1 Introducing the VSG

The VSG (Vantage Service Gateway) allows Internet service providers and property managers to provide broadband Internet access to end users (or subscribers). The VSG is ideal in office or hotspot environments.

Hotspots are public areas, such as airports, hotels, coffee shops, where end users can access the Internet at any time.

1.2 Features

Your VSG provides the following features to accommodate subscribers with a variety of network configurations with little or no technical support.

Plug-and-Play Internet Access

The VSG provides plug-and-play Internet connectivity so subscribers can access the Internet without configuring their computers. In addition, with transparent proxy, the VSG resolves any incompatible proxy settings.

Port Forwarding

Use this feature to forward incoming service requests to a server on your local network.

DHCP Support

DHCP (Dynamic Host Configuration Protocol) allows the individual computers (DHCP clients) to obtain TCP/IP configuration at start-up from a centralized DHCP server. The VSG has built-in DHCP server capability. It can assign IP addresses, an IP default gateway and DNS servers to DHCP clients. The VSG can also act as a surrogate DHCP server (DHCP Relay) where it relays IP address assignment from the actual real DHCP server to the DHCP clients.

RADIUS (Remote Authentication Dial-In User Service) Client

The VSG allows you to maintain a central subscriber database on a remote RADIUS server. Subscriber accounting and authentication is then done through the remote RADIUS server.

CAS (Central Authentication Service)

The Hilton Group Corporation developed the High Speed Internet Access (HSIA) service to provide Internet access service across its entire Hilton Group hotels. In order to use the HSIA, hotel guest(s) must be authenticated through the proprietary CAS. The CAS performs both user authentication and accounting.

Local Subscriber Database

The VSG allows you to maintain a subscriber database on the VSG without setting up an external RADIUS server. Subscriber accounting and authentication are done using the local subscriber database.

Accounting

Accounting can be done using an external RADIUS server or the built-in accounting feature.

Local Content and Advertising Links

Once connected to the network, the VSG directs the subscriber to a specified web site and display advertisement links. This can be a source of extra online advertising revenues and increased business exposure.

Access control (Walled Garden)

With the walled garden feature, subscribers are able to access predetermined web sites without logging in. The VSG blocks full Internet access until the subscribers log in.

E-mail Forwarding

The VSG is able to forward and retrieve e-mail messages when the subscriber's default email server is down or behind a firewall.

DNS Proxy

With DNS proxy, the VSG provides DNS redirection when a subscriber's configured DNS server is behind a firewall or located in a private Intranet.

NAT (Network Address Translation)

NAT (RFC 1631) is the translation of the IP address of a host in a packet, for example, the source address of an outgoing packet, used within one network to a different IP address known within another network.

The VSG automatically performs NAT on the LAN. You may also set the VSG to perform NAT on the WAN for VPN (IPSec and PPTP) connections.

Subscriber Login Page Customization

You can customize the subscriber login page according to your business needs. The advanced settings allows you to include welcome messages, company logo and basic formatting.

Local Console Management

The VSG provides a console port for local management.

Web Configurator Management

The VSG comes with an embedded web-based configurator. It offers advanced management features and allows you to manage the VSG remotely using Internet Explorer (version 5.0 or above) or Netscape Navigator (version 6.0 or above).

Upgrade Firmware via the WAN or Console Port

The firmware of the VSG can be upgraded via the WAN or the console port.

Ease of Installation

Your VSG is designed for quick, intuitive and easy installation. It can be mounted on a desktop or standard 19" rack.

1.3　　Applications

The following sections describe network application examples in which the VSG is used.

1.3.1　　Internet Access for LAN Networks

With a broadband service account set up, the VSG allows the attached computers to enjoy high speed Internet access.
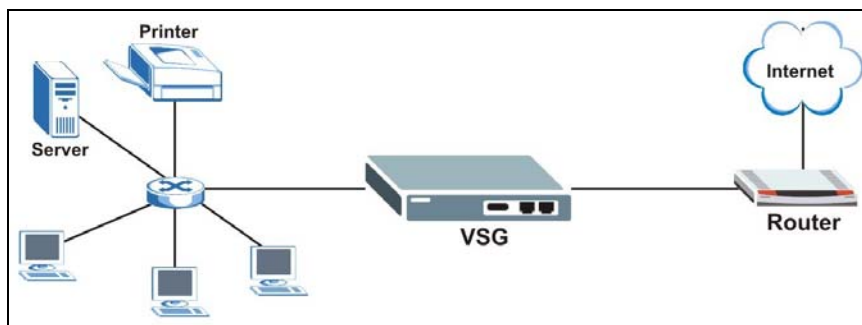
Figure 1-1 Application: Internet Access for LAN Networks

1.3.2   Internet Access in Public Areas

In a hotspot, such as a hotel, the VSG provides high speed Internet access to subscribers. Account billing and authentication can be done either using a remote RADIUS server or the built-in billing function and local subscriber database.

Connect an access point (AP) to bridge the wired and the wireless network allowing wireless stations to access the Internet through the VSG.
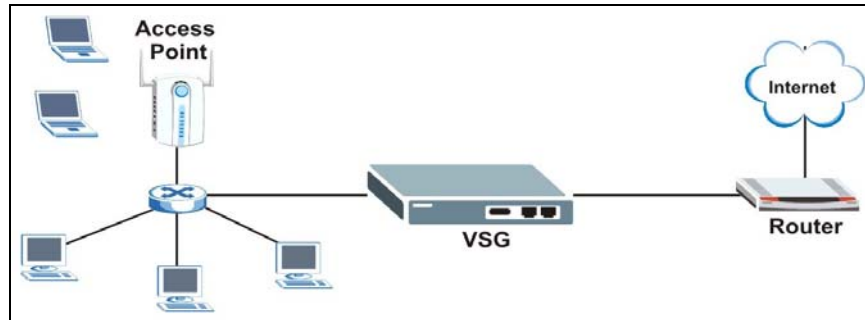
Figure 1-2 Application: Internet Access in Public Areas

Chapter 2
Hardware Installation and Connection

This chapter shows you how to install the VSG and make hardware connections.

2.1 Installation Options

The following sections describe the different installation options.

Do not block the venting holes and leave adequate space on the rear and side of the VSG during hardware installation.

2.1.1 Desktop Installation

Step 1. Make sure the VSG is clean and dry. Set the VSG on a smooth space strong enough to support the weight of the VSG and the connected cables. Make sure there is a power outlet nearby.

Step 2. Make sure there is enough clearance around the VSG to allow air circulation and the attachment of cables and the power cord.

Step 3. Attach the rubber feet to each corner on the bottom of the VSG. These rubber feet help protect the VSG from shock or vibration and ensure space between devices when stacking.

Do not block the ventilation holes. Leave space between devices when stacking.

2.1.2 Rack Mount Installation

The VSG can be mounted on an EIA standard size, 19-inch rack or in a wiring closet with other equipment. Follow the steps below to mount your VSG on a standard EIA rack using the included rack-mounting kit.

Step 4. Align one bracket with the holes on one side of the VSG and secure it with the bracket screws (smaller than the rack-mouting screws. Similarly, attach the other brackets.
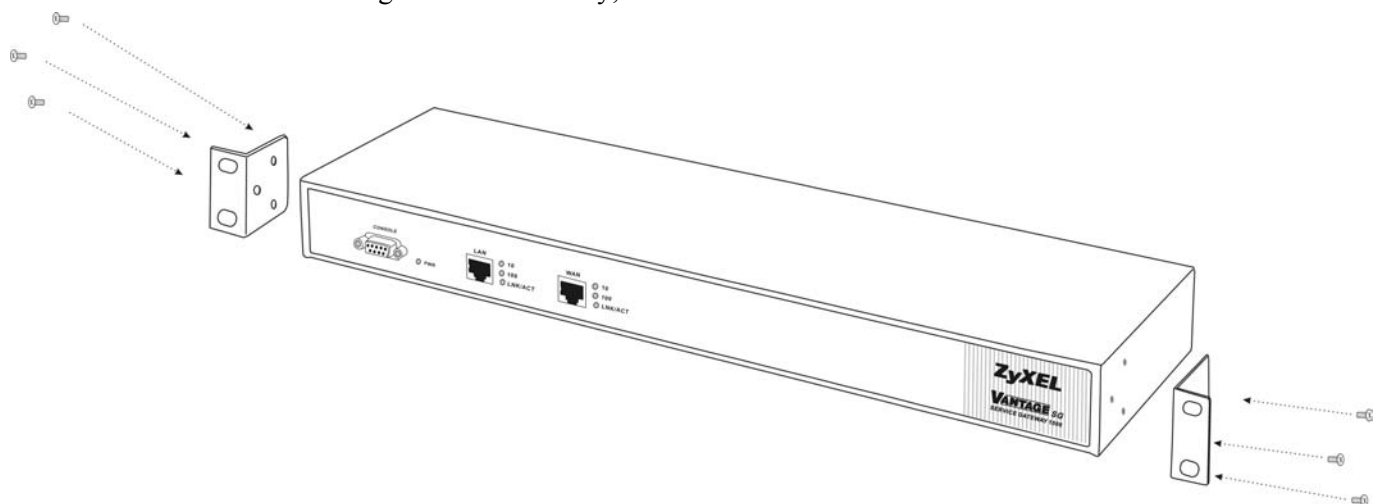
Figure 2-1 Rack Mount: Attaching Brackets

Step 5. After attaching both mounting brackets, position the VSG in the rack by lining up the holes in the brackets with the appropriate holes on the rack. Secure the VSG to the rack with rack-mounting screws.

2.2　Hardware Connections

The following sections describe the hardware connections of the VSG.

2.2.1　Front Panel

The console, LAN and WAN ports and the LEDs are located on the front panel.

Figure 2-2 Front Panel

The LAN Port

Connect the **LAN** port on the VSG to an Ethernet switch or hub using a crossover Ethernet cable or directly to a computer using a straight-through Ethernet cable.

The WAN Port

Connect the VSG to a network with broadband Internet service.

- Connect the **WAN** port to a router using a straight-through Ethernet cable.
- Connect the **WAN** port to a computer using a crossover Ethernet cable for system configuration.

The Console Port

Local management of the VSG is done through the console port. It requires a direct connection between the VSG and a computer via a console cable. Refer to chapters on SMT configurations for more information.

2.2.2　Front Panel LEDs

The following table describes the LEDs on the front panel. All LEDs are green when turned on.

Table 2-1 Front Panel LEDs

LED	STATUS	DESCRIPTION
PWR	On	The VSG is receiving power.
	Off	The VSG is not receiving power.
LAN or WAN		
LINK 10	On	The port is operating at 10Mpbs.
	Off	No device is connected at 10Mpbs.
LINK 100	On	The port is operating at 100Mbps.
	Off	No device is connected at 100 Mbps.
ACT	On	The port is receiving or sending data.
	Blinking	The port is receiving or sending data.

2.2.3　Rear Panel

The power socket, the fan and a ventilation hole are located on the rear panel as shown next.
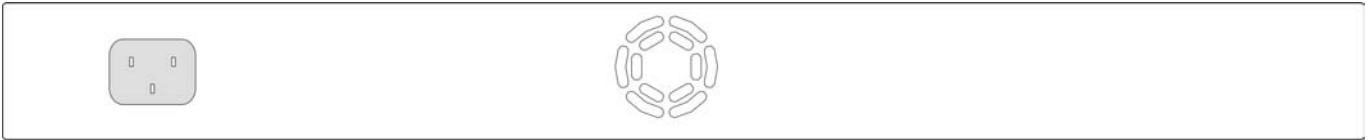
Figure 2-3 Rear Panel

2.2.4 Turning on the VSG

Connect one end of the supplied power cord to the power socket on the back of the VSG and the other end to an appropriate power source.

When the power source is turned on, the **PWR** LED on the front panel turns on.

Chapter 3
The Web Configurator

This chapter introduces how to access the web configurator and perform general system configuration.

3.1 Introducing the Web Configurator

The web configurator is best viewed with Internet Explorer (version 5.0 or above) or Netscape (version 6.0 or above) with JavaScript support enabled.

3.2 Accessing the Web Configurator

All web configurator screens are shown in Internet Explorer. Follow the steps below to access the web configurator.

You must access the web configurator through the WAN.

The VSG allows only one login session at any one time using the web configurator.

Step 1. Make sure your VSG is properly connected (refer to instructions in the chapter on hardware installtion).

Step 2. Launch your web browser and type the WAN IP address (192.168.1.1 is the default) of the VSG as the web address.
If you are using a different port number (between 8000 and 8099) for the web server, you must also append the port number to the WAN IP address seperated with a colon ":",for example, http://192.168.1.1:8080.
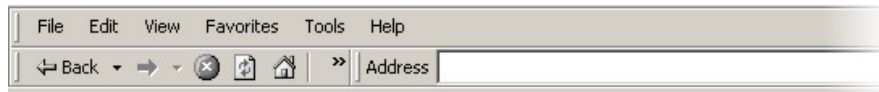
Figure 3-1 Entering VSG IP Address in Internet Explorer

Step 3. A login screen displays. The firmware version number is displayed in the login screen. Type "admin" (default) as the user name and "1234" (default) as the password and click **Enter**.

The user name and password are case sensitive.

Figure 3-2 Web Configurator: Login

Step 4. You should see the main screen as shown.
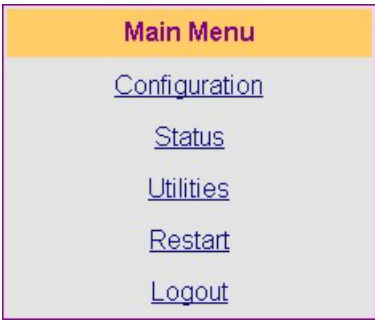
Figure 3-3 Web Configurator: Main Menu

Please note that if there is no activity for longer than 5 minutes after you log in, the VSG will automatically log you out. If this happens, simply log back in again.

3.3 System Login Accounts

You can use two different system accounts (administrator and account manager) to log into the web configuration.

The administrator account allows you full access to all system configuration. The default user name is "admin" and password "1234". Refer to the *Troubleshooting* chapter if you forget the administrator username and/or password.

The account manager account is used for subscriber account management only. No system configuration is allowed. This account is useful for front desk personnel (such as in a hotel) for setting up subscriber accounts without tampering with the system configuration. The default user name and password is "account".

3.4 Changing System Password

It is recommended you change the system passwords.
You can only change the account manager account password in the web configurator.

From the **Main Menu** screen, click **Utility** and **Change Password**.

Figure 3-4 Web Configurator: Changing System Password

The following table describes the labels in this screen.

Table 3-1 Web Configurator: Changing System Password

LABEL	DESCRIPTION
Change Administrator Password	
Old Password	Enter the existing administrator password.
New Password	Enter a new administrator password.
New Password (confirm)	Enter the new administrator password again for confirmation.
Change Account Manager Password	
Old Password	Enter the existing account manager password.
New Password	Enter the new account manager password.
New Password (confirm)	Enter the new account manager password again for confirmation.
Apply	Click **Apply** to save the changes back to VSG and go back to the **Utility Menu**.
Clear	Click **Clear** to start configuring this screen again.
Home	Click **Home** to go back to the **Main Menu** screen. The changes you made will not be saved if you have not clicked **Apply**.
Previous	Click **Previous** to go back to the previous screen. The changes you made will not be saved if you have not clicked **Apply**.

3.5 Restarting the VSG

You *must* restart the VSG every time you change the system IP address or uploads a firmware or configuration file.

In the **Main Menu** screen, click **Restart** and then the **Restart** button.
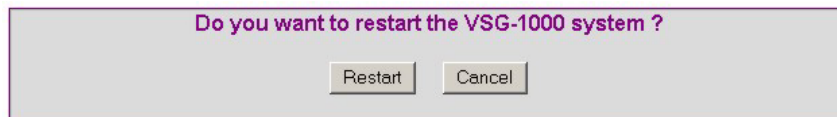
Figure 3-5 Web Configurator: Restarting

3.6 Logging Out of the Web Configurator

In the **Main Menu** screen, click **Logout** and the **Logout** button to exit from the web configurator.
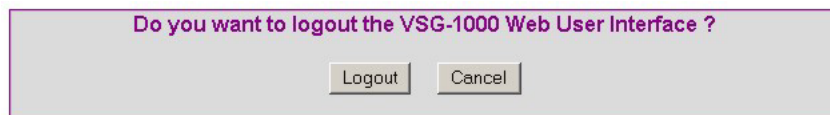
Figure 3-6 Web Configurator: Logging Out

Part II:

Web Configurator System Configuration

This part covers system configuration and subscriber management using the web configurator.

Chapter 4
System Configuration

This chapter shows you how to configure the network settings of the VSG.

4.1 Factory Ethernet Defaults

The Ethernet parameters of the VSG are preset to the following values:

1. WAN IP address of 192.168.1.1 with subnet mask of 255.255.255.0 and default gateway of 192.168.1.254.
2. LAN IP address of 10.59.1.1 with subnet mask of 255.255.255.0 (24 bits).
3. DHCP server enabled on the LAN with a 252 client IP address pool starting from 10.59.1.2

These parameters should work for the majority of installations. If you wish to change the factory defaults or to learn more about TCP/IP, please read on.

4.2 LANs and WANs

A LAN (Local Area Network) is a computer network limited to the immediate area, usually the same building or floor of a building. A WAN (Wide Area Network), on the other hand, is an outside connection to another network or the Internet.

4.3 IP Address Assignment

A static IP is a fixed IP that the VSG obtains from a DHCP server on a network. A dynamic IP is not fixed; the DHCP server provides an IP address to the VSG each time it connects to the network. When an Ethernet device is configured to obtain a dynamic IP address from a DHCP server, it is known as a DHCP client.

4.4 DHCP Configuration

DHCP (Dynamic Host Configuration Protocol) allows the individual clients (Ethernet device) to obtain the TCP/IP configuration at start-up from a centralized DHCP server. The VSG has built-in DHCP server capability, which means it can assign IP addresses, an IP default gateway and DNS servers to computer systems that support the DHCP client when this feature is activated. The VSG can also act as a surrogate DHCP server where it relays IP address assignment from the actual DHCP server to the clients.

4.4.1   IP Address and Subnet Mask

Like houses on a street that share a common street name, the computers on a LAN share one common network number.

Where you obtain your network number depends on your particular situation. If the ISP or your network administrator assigns you a block of registered IP addresses, follow their instructions in selecting the IP addresses and the subnet mask.

The Internet Assigned Number Authority (IANA) reserved a block of addresses specifically for private use (refer to *Section 4.4.2*); please do *not* use any other number unless you are told otherwise. Let's say you select 192.168.1.0 as the network number; which covers 254 individual addresses, from 192.168.1.1 to 192.168.1.254 (zero and 255 are reserved). In other words, the first three numbers specify the network number while the last number identifies an individual computer on that network.

The subnet mask specifies the network number portion of an IP address.

4.4.2　　　Private IP Addresses

Every machine on the Internet must have a unique address. If your networks are isolated from the Internet, for example, only between your two branch offices, you can assign any IP addresses to the hosts without problems. However, the Internet Assigned Numbers Authority (IANA) has reserved the following three blocks of IP addresses specifically for private networks:

```
10.0.0.0     —  10.255.255.255

172.16.0.0   —  172.31.255.255

192.168.0.0  —  192.168.255.255
```

You can obtain your IP address from the IANA, from an ISP or it can be assigned from a private network. If you belong to a small organization and your Internet access is through an ISP, the ISP can provide you with the Internet addresses for your local networks. On the other hand, if you are part of a much larger organization, you should consult your network administrator for the appropriate IP addresses.

Regardless of your particular situation, do not create an arbitrary IP address; always follow the guidelines above. For more information on address assignment, please refer to RFC 1597, *Address Allocation for Private Internets* and RFC 1466, *Guidelines for Management of IP Address Space.*

4.5　DNS Server Address

DNS (Domain Name System) is for mapping a domain name to its corresponding IP address and vice versa, for example, the IP address of *www.zyxel.com* is 204.217.0.2. The DNS server is extremely important because without it, you must know the IP address of a machine before you can access it. The DNS server addresses that you enter in the DHCP setup are passed to the client machines along with the assigned IP address and subnet mask.

There are two ways that an ISP disseminates the DNS server addresses. The first is for an ISP to tell a customer the DNS server addresses, usually in the form of an information sheet, when s/he signs up. The second is to obtain the DNS server information automatically when a computer is set as a DHCP client.

4.6　Syslog

Your VSG sends logs to an external server used to store logs. The logs contain the current user information such as the MAC address and IP address. The syslog format is as follows.

```
Log format: <166 Information>
```
```
[System Time yy/mm/dd/hh/mm/ss, System IP, System Name, username1, user's IP,
user's MAC, username2…]
```

Refer to *Table 4-7* for descriptions of system logs you may select in the **System Configuration** screen.

4.7　NAT

NAT (Network Address Translation - NAT, RFC 1631) is the translation of the IP address of a host in a packet, for example, the source address of an outgoing packet, used within one network to a different IP address known within another network.

4.7.1　　　NAT Definitions

Inside/outside denotes where a host is located relative to the VSG, for example, the computers of your subscribers are the inside hosts, while the web servers on the Internet are the outside hosts.

Global/local denotes the IP address of a host in a packet as the packet traverses a router, for example, the local address refers to the IP address of a host when the packet is in the local network, while the global address refers to the IP address of the host when the same packet is traveling in the WAN side.

Note that inside/outside refers to the location of a host, while global/local refers to the IP address of a host used in a packet. Thus, an inside local address (ILA) is the IP address of an inside host in a packet when the packet is still in

the local network, while an inside global address (IGA) is the IP address of the same inside host when the packet is on the WAN side. The following table summarizes this information.

Table 4-1 NAT Definition

ITEM	DESCRIPTION
Inside	This refers to the host on the LAN.
Outside	This refers to the host on the WAN.
Local	This refers to the packet address (source or destination) as the packet travels on the LAN.
Global	This refers to the packet address (source or destination) as the packet travels on the WAN.

NAT never changes the IP address (either local or global) of an outside host.

4.7.2   What NAT Does

In the simplest form, NAT changes the source IP address in a packet received from a subscriber (the inside local address) to another (the inside global address) before forwarding the packet to the WAN side. When the response comes back, NAT translates the destination address (the inside global address) back to the inside local address before forwarding it to the original inside host. Note that the IP address (either local or global) of an outside host is never changed.

The global IP addresses for the inside hosts can be either static or dynamically assigned by the ISP. In addition, you can designate servers, for example, a web server and a telnet server, on your local network and make them accessible to the outside world. If you do not define any servers, NAT offers the additional benefit of firewall protection. With no servers defined, your VSG filters out all incoming inquiries, thus preventing intruders from probing your network. For more information on IP address translation, refer to *RFC 1631, The IP Network Address Translator (NAT)*.

4.7.3   How NAT Works

Each packet has two addresses – a source address and a destination address. For outgoing packets, the ILA (Inside Local Address) is the source address on the LAN, and the IGA (Inside Global Address) is the source address on the WAN. For incoming packets, the ILA is the destination address on the LAN, and the IGA is the destination address on the WAN. NAT maps private (local) IP addresses to globally unique ones required for communication with hosts on other networks. It replaces the original IP source address in each packet and then forwards it to the Internet. The VSG keeps track of the original addresses and port numbers so incoming reply packets can have their original values restored.

4.7.4   VPN and NAT

A VPN (Virtual Private Network) provides secure communications between sites without the expense of leased site-to-site lines. A secure VPN is a combination of tunneling, encryption, authentication, access control and auditing technologies/services used to transport traffic over the Internet or any insecure network that uses the TCP/IP protocol suite for communication.

The VSG allows subscribers to create a VPN tunnel to a remote site. By default, the VSG performs NAT on the LAN; mapping multiple private LAN addresses to a single public address on the WAN. This prevents subscribers from creating multiple VPN connections to a remote VPN device that allows only one VPN connection per source IP address.

For IPSec, the VSG does not support AH protocol.

In order to allow subscribers to establish multiple VPN connections to a remote VPN device with single-connection-per-source limitation, set the VSG to perform NAT on the WAN. You need to configure NAT address

pool for use with VPN connections on the WAN port. The VSG automatically maps one/more private IP addresses to one/more public IP addresses for VPN packets. The following table describes the NAT mapping types on the WAN for VPN packets.

Table 4-2 WAN NAT Mapping Type For VPN

TYPE	DESCRIPTION
One-to-One	For VPN connections to the same remote VPN device, the VSG maps each private LAN IP address to one public WAN IP address.
One-to-Many	For VPN connections to different remote VPN devices, the VSG maps multiple private LAN IP address to one public WAN IP address.

4.7.5   NAT Examples

The following sections describe some NAT address mapping examples for VPN connections.

Example 1: One-to-One

The figure below shows an example where the two subscribers **S1** and **S2** tries to establish secure VPN connections to the same VPN server **V1** at the same time. For example, the VSG is using a public IP address of 211.21.21.1[1]. In this case, the VSG performs One-to-One IP address translation on the WAN.
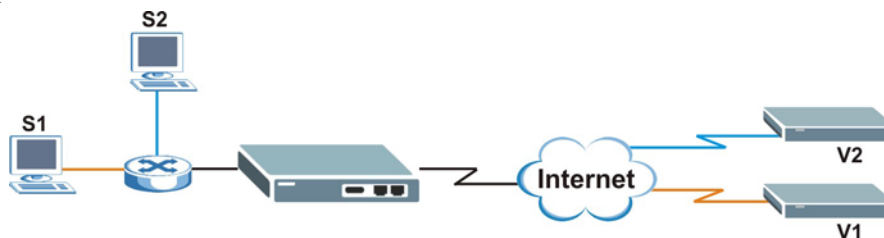
Figure 4-1 NAT Example: One-to-One

The following table shows the address mapping.

Table 4-3 NAT Example: One-to-One

SUBSCRIBER	ORIGINAL SOURCE IP	TRANSLATED SOURCE IP
S1	10.59.1.2	211.21.21.2
S2	10.59.1.3	221.21.21.3

Example 2: Many-to-One

The figure below shows an example where the two subscribers **S1** and **S2** try to establish a secure VPN connection to VPN servers **V1** and **V2** respectively at the same time. In this case, the VSG performs Many-to-One IP address translation on the WAN since the destination address is different.
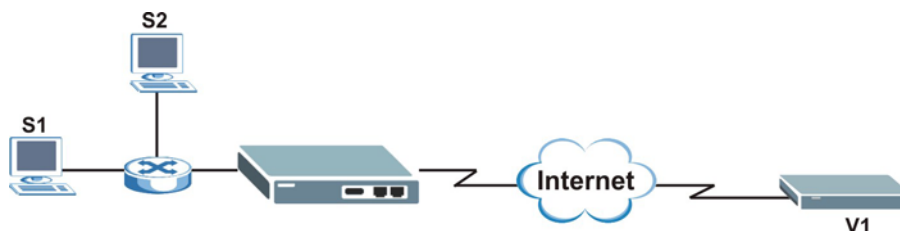
Figure 4-2 NAT Example: Many-to-One

The following table shows the address mapping.

---

[1] All public IP address discussed are for examples only.

Table 4-4 NAT Example: Many-to-One

SUBSCRIBER	ORIGINAL SOURCE IP	TRANSLATED SOURCE IP
S1	10.59.1.2	211.21.21.2
S2	10.59.1.3	221.21.21.2

Example 3: One-to-One and Many-to-One

The figure below shows an example where subscriber **S1** tires to connect to VPN server **V1** while subscriber **S2** and **S3** try to connect to the same VPN server **V2** at the same time. In this case, subscribers **S1** and **S2** map to the same WAN IP address since the destination is different while subscriber **S3** maps to a different WAN IP address.
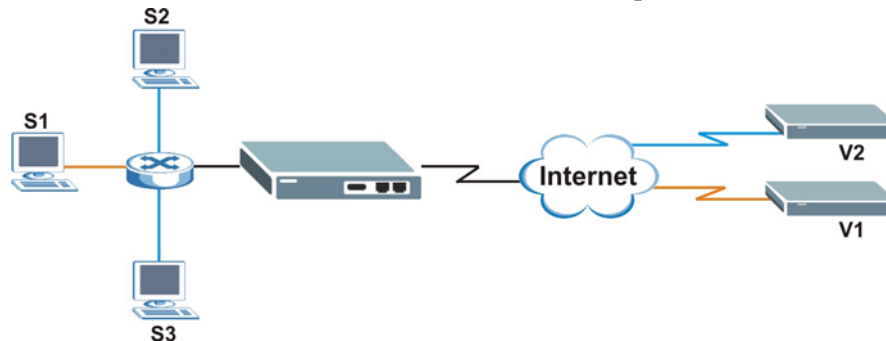
Figure 4-3 NAT Example: One-to-One and Many-to-One

The following table shows the address mapping.

Table 4-5 NAT Example: One-to-One and Many-to-One

SUBSCRIBER	ORIGINAL SOURCE IP	TRANSLATED SOURCE IP
S1	10.59.1.2	211.21.21.2
S2	10.59.1.3	221.21.21.2
S3	10.59.1.4	221.21.21.3

You only need to set the NAT address pool if the remote VPN server(s) allows only one connection per source IP address.

You need to acquire additional public IP address(es) from your ISP to create NAT pool(s).

4.8 The System Configuration Screen

From the **Main Menu** screen, click **Configuration** and **System** to display the screen as shown.

Figure 4-4 System Configuration

The following table describes the fields in this screen.

Table 4-6 System Configuration

LABEL	DESCRIPTION
System Name	Enter a descriptive name for identification purposes.
Console Port Speed	Select the console port speed from the drop-down list box. Choices are **9600**, **19200** and **38400**. The default setting is **9600**.
	If you change the console port speed, make sure you also make the same change to the terminal emulator software.
Administration Idle-Timeout	Specify how many minutes (between 1 and 1440) the web configuration can be left idle before the session times out. After it times out you have to log in with your password again. Very long idle timeouts may have security risks. The default is **5** minutes.
	This does *not* apply to the SMT.
User Session Limit	Use this field to limit how many session connections per subscriber. Select **10**, **20**, **40**, **80**, **160**, **320**, or **640**. Select **UnLimited** to not impose a restriction on the number of session connections per subscriber.
Date/Time	Set the system date and time by selecting the appropriate choices from the drop-down list boxes.
WAN Set the following fields for the **WAN** port on the VSG.	
DHCP Client	Select this option to set the VSG to obtain an IP address and other network information from a DHCP server on the network.
Static IP Setting	Select this option to configure the VSG to use a static (fixed) IP address. Then set the following fields.
Specify IP Address	Enter the static WAN IP address assigned to you by your ISP or network administrator.
Subnet Mask	Enter the subnet mask depending on your network needs. The default is **255.255.255.0**. Refer to the *Subnetting* appendix if you are implementing subnetting.
Default Gateway	Enter the IP address of the default gateway.
Web Server Port	Specify the port number of the embedded web server on the VSG to access the web configurator. The default port number is **80**. Enter a number between 8000 and 8099 to access the web configurator behind a NAT-enabled network. If you enter a number between 8000 and 8099, you need to append the port number to the **WAN** port IP address to access the web configurator. For example, if you enter "8000" as the web server port number, then you must enter "http://www.192.168.1.1:8000" where 192.168.1.1 is the WAN port IP address.
DHCP Configuration Set the following fields for the **LAN** port on the VSG.	
DHCP Disable	Select this option to deactivate the DHCP server function on the VSG.
DHCP Relay	Select this option to set the VSG to forward network configuration requests to a DHCP server on the network. Then set the following fields (not shown in the figure).
DHCP Server IP Address	Enter the IP address of the DHCP server.
DHCP Agent IP Address	Enter the IP address of the DHCP relay agent. In most cases, this is the WAN IP address of the VSG.
DHCP Server	Select this option to set the VSG to act as a DHCP server. Then set the following fields.
DHCP Server IP Address	Enter the LAN IP address of the VSG.
DHCP Pool Start IP Address	Enter the first of the contiguous addresses in the IP address pool.

Table 4-6 System Configuration

LABEL	DESCRIPTION
DHCP Pool End IP Address	Enter the first of the contiguous addresses in the IP address pool.
DHCP Subnet Mask	Enter the subnet mask based on the IP address you specified in the **DHCP Server IP Address**, **DHCP Pool Start IP Address** and **DHCP Pool End IP Address** fields. Refer to the *Subnetting* appendix if you are implementing subnetting.
Lease Time Duration Minutes	Specify the time (in minutes between 1 and 71582788) a DHCP client is allowed to use an assigned IP address. When the lease time expires, the DHCP client is given another IP address. The maximum is 71582788 minutes.
Email Server	Enter the domain name or IP address of the e-mail server to which the VSG forwards the emails. This field should be configured if the e-mail server is behind a firewall or on a NAT-enabled network.
DNS	Enter the IP address of the DNS server(s) in the **Primary IP Address** and/or **Secondary IP Address** fields. **You *must* specify a DNS server.**
Backup Billing Subscribers	Select **Enable** to back up subscriber Internet usage information every five minutes. This helps prevent data lose due to unexpected power disruptions. Once the VSG restarts, the VSG automatically restores the subscriber Internet usage information. Select **Disable** to deactivate this feature. No subscriber Internet usage information is retained.
Syslog	
Enable/Disable	Select **Enable** to activate syslog logging. Select **Disable** to deactivate syslog logging.
Primary Server IP	Enter the IP address of the primary syslog server to which the logs are sent.
Secondary Server IP	Enter the IP address of the secondary syslog server to which the logs are sent.
Interval Time	Enter the time interval (in minutes) to wait between sending any logs to the syslog servers specified in the **Primary Server IP** and **Secondary Server IP** fields. The maximum allowable time interval is **10080** minutes. Enter **0** to disable this feature. This is the default setting.
System Boot Notice	Select this checkbox to set the VSG to send a log after the system startup process.
System and Logged-in User Information Every (Min)	Select this checkbox to set the VSG to send a log with system and current logged-in user information every time interval specified.
System Manager Activity Information	Select this checkbox to set the VSG to send a log every time the system administrator/account manager logs in/out.
NAT Pool Exhausted Notice	Select this checkbox to set the VSG to send a log when one or all configured WAN IP address(es) is already used for VPN connection NAT.
NAT Pool	
You only need to set the NAT address pool if the remote VPN server(s) allows only one connection per source IP address. **You need to acquire additional public IP address(es) from your ISP to create NAT pool(s).**	
Enable/Disable	Select **Enable** to perform address translation on the WAN to allow subscribers to establish simultaneous connections to the same VPN server (that has the single-connection-per-source limitation). You must then configure the address pool for VPN connections. Select **Disable** to deactivate this feature. Subscribers are not be able to establish multiple connections simultaneously to the same VPN server (that has the single-connection-per-source limitation).
No	This field displays the index number.

Table 4-6 System Configuration

LABEL	DESCRIPTION
Public Address List	Specify the beginning and ending IP addresses of the address pool in the fields provided.
	You can configure up to five address pools on the VSG.
	Make sure the total number of addresses in the address pool does not exceed 50.
	The following shows three NAT pool examples if the VSG is using a WAN public IP address of 211.21.21.1:
	Group 1: 211.21.21.2 ~ 211.21.21.6 (five IP addresses)
	Group 2: 211.21.21.20 ~ 211.21.21.29 (ten IP addresses)
	Group 3: 211.21.21.60 ~ 211.21.21.69 (ten IP addresses)
	Group 4: 211.21.21.75 ~ 211.21.21.76 (two IP addresses)
Apply	Click **Apply** to save the changes back to VSG and go back to the **Utility Menu**.
Clear	Click **Clear** to start configuring this screen again.
Home	Click **Home** to go back to the **Main Menu** screen. The changes you made will not be saved if you have not clicked **Apply**.
Previous	Click **Previous** to go back to the previous screen. The changes you made will not be saved if you have not clicked **Apply**.

The following table describes the system logs you may select in the **System Configuration** screen.

Table 4-7 Syslog Description

TYPE	LOG FORMAT	DESCRIPTION
System Boot Notice	Date/Time)(SystemName)(**Id**, Mac Address)(**System Up**)	This log is sent every time the VSG reboots successfully.
System Information	(**Id**, Mac Address) (**System Uptime**, 0 days 00h:04m:00s, System IP 120.1.1.1, System name,) (**Logged-in Users**, Number of logged-in users, Start Number, End number) (Username, user IP, user MAC)(…)(…)	A log with system and currently logged-in user information is sent every time interval specified. Default time interval is 60 minutes.
System Manager Activity Information	(Date/Time)(SystemName)(**Id**, Mac Address) (**System Manager Activity Information**, Username, User IP, Status)Username : **Administrator** | **Account Manager**Status : **Login** | **Logout** | **Idle Time Out** | **Login Fail**	This log records the access information of a system account (administrator or account manager).
NAT Pool Exhausted Notice	(Date/Time)(SystemName)(**Id**, Mac Address)(**NAT Pool Exhausted,** type) Type: IP / Port	This log is sent when all public WAN IP address(es) is used for VPN NAT.

Chapter 5
Subscriber Control

*This chapter shows you how to use the **Subscriber Control** screen to set up subscriber account information and authentication method.*

5.1 Overview

By default, subscriber authentication is disabled. This allows all subscribers to access the Internet without entering account username and password.

5.1.1   Activating Subscriber Control

Set the subscriber authentication settings in the **Subscriber Management** screen. From the main screen, click **Configuration**, **Subscriber Management** and **Subscriber Control**.

Figure 5-1 Subscriber Control: Activation

The following table describes the **Subscriber Control** fields in this screen.

Table 5-1 Subscriber Control: Activation

FIELD	DESCRIPTION
Subscriber Control	
Enable	Select **Enable** to activate subscriber authentication and configure the related fields as described in the following sections.
Disable	Select **Disable** to allow subscribers Internet access without logging in.
Idle-Timeout	The VSG automatically disconnects a computer from the network after a period of inactivity. The subscriber may need to enter the username and password again before access to the network is allowed. Specify the idle timeout between 1 and 1440 minutes. The default is 30 minutes.
Apply	Click **Apply** to save the changes back to VSG and go back to the **Utility Menu**.
Clear	Click **Clear** to start configuring this screen again.
Home	Click **Home** to go back to the **Main Menu** screen. The changes you made will not be saved if you have not clicked **Apply**.
Previous	Click **Previous** to go back to the previous screen. The changes you made will not be saved if you have not clicked **Apply**.

5.2 Management Type

You can set the VSG to authenticate subscriber in a number of ways:

- ➢ User agreement
- ➢ CAS (Central Authentication Service)
- ➢ Built-in authentication
- ➢ Remote RADIUS server

5.2.1 Super User Account

For built-in and remote RADIUS authentication methods, you can set up a super user account. This account is useful for testing the Internet connection from the LAN through the VSG. The super user account allows multiple logins but no system configuration is allowed.

Anyone using the super user account can get Internet connectivity for free as no billing mechanism or time limitation is imposed.

5.2.2 User Agreement

In cases where authentication is not required and anyone can access the Internet through the VSG, you can set the VSG to redirect client users to an Internet service usage agreement page.

Users *must* accept the service usage agreement before they can access the Internet.

Display the **Subscriber Control** screen as shown.

Figure 5-2 Subscriber Control: User Agreement

The following table describes the labels in this screen.

Table 5-2 Subscriber Control: User Agreement

LABEL	DESCRIPTION
Subscriber Control	Select **User Agreement** to direct a subscriber to an Internet service usage agreement page before accessing the Internet.
Redirect Page URL Link	Specify the URL of the user agreement page in the field provided. Click **Code** to display the HTML source code of a sample page.
Idle-Timeout	The VSG automatically disconnects a computer from the network after a period of inactivity. The subscriber may need to enter the username and password again before access to the network is allowed. Specify the idle timeout between 1 and 1440 minutes. The default is 30 minutes.
Apply	Click **Apply** to save the changes back to VSG and go back to the **Utility Menu**.
Clear	Click **Clear** to start configuring this screen again.
Home	Click **Home** to go back to the **Main Menu** screen. The changes you made will not be saved if you have not clicked **Apply**.

Table 5-2 Subscriber Control: User Agreement

LABEL	DESCRIPTION
Previous	Click **Previous** to go back to the previous screen. The changes you made will not be saved if you have not clicked **Apply**.

5.2.3   CAS (Central Authentication Service)

The Hilton Group Corporation developed the High Speed Internet Access (HSIA) service to provide Internet access service across its entire Hilton Group hotels. In order to use the HSIA, hotel guest(s) must be authenticated through the proprietary CAS. The CAS performs both user authentication and accounting.
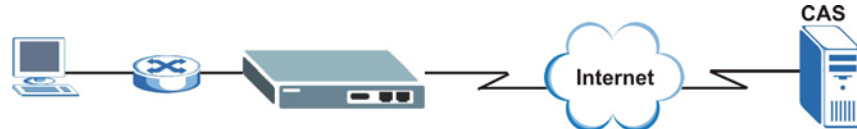
Figure 5-3 CAS Example

The following summarizes the communication steps before Internet access is allowed.

Step 1.   A hotel guest launches a web browser.

Step 2.   The VSG redirects the guest's web browser to a login screen at CAS.

Step 3.   The guest enters the provided access information.

Once authentication is successful, CAS informs VSG to allow Internet access to the guest.

Figure 5-4 Subscriber Control: CAS

The following table describes the related labels in this screen.

Table 5-3 Subscriber Control: CAS

LABEL	DESCRIPTION
Subscriber Control	Select **CAS (Hilton HSIA)** to use the Hilton Group proprietary CAS (Central Authentication Service) for HSIA. Then specify the fields below.
Gateway Type	Specify the type of this gateway from the drop-down list box. Select **ZYL** for ZyXEL devices. Otherwise, select **GEN**.
Property Code	Enter the provided property location code (up to five characters) for the hotel. This identifies the location of the Internet access request.
Property Zip	Enter the provided property zip code (between four and 10 characters).

Table 5-3 Subscriber Control: CAS

LABEL	DESCRIPTION
Redirect URL	Specify the web site address of the login screen to which the hotel guests are directed for authentication using CAS.
	Enter the web site address as provided by the Hilton HSIA support team.
Apply	Click **Apply** to save the changes back to VSG and go back to the **Utility Menu**.
Clear	Click **Clear** to start configuring this screen again.
Home	Click **Home** to go back to the **Main Menu** screen. The changes you made will not be saved if you have not clicked **Apply**.
Previous	Click **Previous** to go back to the previous screen. The changes you made will not be saved if you have not clicked **Apply**.

5.2.4 Built-in Authentication

You can use the local subscriber database on the VSG to set up subscriber information. This is useful if you don't have a RADIUS server.

Billing Mechanism

When you select **Built-in Authentication** as the management type in the **Subscriber Control** screen, the VSG provides a simple built-in billing mechanism that allows you to set up accounting information without using accounting software or using an accounting server (such as RADIUS).

The billing mechanism does not apply to the super user account.

Figure 5-5 Subscriber Control: Built-in Authentication

The following table describes the built-in authentications management type fields in this screen.

Table 5-4 Subscriber Control: Built-in Authentication

FIELD	DESCRIPTION
Management Type	Select **Built-in Authentication** to use the local subscriber database on the VSG.

Table 5-4 Subscriber Control: Built-in Authentication

FIELD	DESCRIPTION
Super User Account	Select **Enable** from the drop-down list box to activate the super user account. Refer to the *Super User Account* section for more information.
Username	Enter the username for the super user account.
Password	Enter the password for the super user account.
Billing Mechanism	Select **Enable** to activate this feature and set the following fields. Select **Disable** to de-activate this feature. This is the default setting. Subscribers can connect to the Internet without time limitation.
Unit Time	Select the time interval of a unit. Choices are **by Day** and **by Hour**.
Unit Cost	Enter the cost of a unit.
Currency	Enter the type of currency, for example, US.

5.2.5   RADIUS

The VSG supports Remote Authentication Dial-In user Service (RADIUS). By integrating RADIUS with the VSG, you can set up the subscriber database on the RADIUS server. In addition to subscriber information, the subscriber database may hold the Internet usage time period each subscriber is allocated. For example, when a subscriber logs in, the RADIUS server will send the time allocation information (such as session time-out) to the VSG, which uses this information to control subscriber's connection.

Accounting Method

The VSG sends "accounting start" and "accounting stop" messages to the RADIUS server, which uses these messages to accurately track subscriber Internet usage.

The VSG provides two accounting methods: **Accumulation** and **Time to Finish**.

The **Accumulation** accounting method allows multiple re-logins until the allocated time period or until the subscriber account is invalid. The VSG accounts for the time the subscriber logs in for Internet access.

The **Time to Finish** accounting method is good for one-time logins. Once a subscriber logs in, the VSG stores the MAC address of the subscriber's computer for the duration of the time allocated. Thus the subscriber does not have to enter the user name and password again for re-login within the allocated time. Once activated, the subscriber account is valid until the allocated time is reached even if the subscriber disconnects Internet access for a certain period within the allocated time. For example, if Joe purchases a one-hour time-to-finish account. He starts using the Internet for the first 20 minutes and then disconnects Internet access to go to a 20-minute meeting. Then he only has 20 minutes left on his account.

Subscriber Pop-up Logout Window

Enable this feature to automatically display a popup window on a subscriber's computer after a successful login. This popup window displays time usage information and may allow a subscriber to terminate the Internet connection. Refer to *Section 5.2.6* for more information and screen examples.

Online Sign Up

With the RADIUS management type, you can set up an automatic online sign-up option that allows a subscriber to purchase an Internet access account online using a credit card. You must specify a secure web site where the subscriber can enter the credit card information. This secure web site address displays on the sign-up screen and the subscriber is allowed to access the web site temporarily without authentication.

In the **Subscriber Control** screen, select **Radius** to display the screen as shown next.

Figure 5-6 Subscriber Control: RADIUS

The following table describes the RADIUS-related fields in the **Subscriber Control** screen.

Table 5-5 Subscriber Control: RADIUS

FIELD	DESCRIPTION
Management Type Select **RADIUS** to use the subscriber database on a remote RADIUS server.	
Primary Server	
Server IP	Enter the IP address of the primary authentication server in dotted decimal notation.
Authentication Port	Specify the authentication port of the primary RADIUS server. The common port numbers are 1645 and 1812.

Table 5-5 Subscriber Control: RADIUS

FIELD	DESCRIPTION
Accounting Port	Specify the accounting port of the primary RADIUS server. The common port numbers are 1646 and 1813.
Secret Key	Specify a password (up to 31 alphanumeric characters) as the key to be shared between the primary RADIUS server and the VSG. The key is not sent over the network. This key must be the same on the primary RADIUS server and the VSG.
Secondary Server	
Server IP	Enter the IP address of the secondary authentication server in dotted decimal notation.
Authentication Port	Specify the authentication port of the secondary RADIUS server. The common port numbers are 1645 and 1812.
Accounting Port	Specify the accounting port of the secondary RADIUS server. The common port numbers are 1646 and 1813.
Secret Key	Specify a password (up to 31 alphanumeric characters) as the key to be shared between the secondary RADIUS server and the VSG. The key is not sent over the network. This key must be the same on the secondary RADIUS server and the VSG.
RADIUS Common Settings	
Accounting Type	Select **Accumulation** for multiple re-login until the time allocated is used up. If a subscriber logs out and access the Internet again within the time period specified in the **Idle Timeout** field, the subscriber does not have to enter the user name and password again to log in. Select **Time to Finish** to allow one-time login.
Accounting Service	Select **Enable** from the drop-down list box to activate the accounting feature. Otherwise, select **Disable** to de-activate the accounting feature.
Authentication Method	Select either the **CHAP** or **PAP** authentication method from the drop-down list box.
Transmission Attempts	Specify the number of times (1 to 3) the VSG resends an authentication request to the primary and/or secondary RADIUS servers.
Pop-up Logout Window	Select **Enable** to automatically displays a pop-up window after a successful login. This window displays either the remaining time or the time used, depending on the accounting type and the RADIUS server setting. Select **Disable** to not display the pop-up window automatically. See *Section 5.2.7* on how to open the pop-up window manually if applicable.
Super User Account	Select **Enable** from the drop-down list box to activate the super user account. Refer to the *Super User Account* section for more information.
Username	Enter the username for the super user account.
Password	Enter the password for the super user account.
On Line Sign Up Select **Enable** to activate this feature and set the following fields.	
Connection Duration Min(s) (1-1440)	Specify how long a subscriber is allowed to access the web site for entering credit card information before Internet access is disconnected. Enter the time interval between 1 and 1440 minutes.
Account Server IP/Domain Name	Enter the IP address or domain name of the subscriber account server.
URL	Enter the web site address of the secure web site for entering credit card information.

5.2.6 Subscriber Pop-up Logout Window

When this feature is activated for RADIUS management type, the pop-up logout window displays how long the subscriber has accessed or has yet to access the Internet depending on the accounting method you select and the remote RADIUS server settings. When a subscriber terminates the Internet connection, a message is sent to the RADIUS server to stop the accounting process and update the accounting information.

The following table summarizes the different logout windows and the configuration options in the **Subscriber Control** screen. When applicable, a subscriber clicks **Logout** to terminate the Internet connection and log out.

Table 5-6 Subscriber Pop-up Logout Windows Variations

ACCOUNTING TYPE FIELD	RADIUS SERVER SESSION TIMEOUT MESSAGE	LOGOUT WINDOW EXAMPLE
Time to Finish	Yes	**Figure 5-7 Subscriber Logout Window: Version 1**
Accumulation	Yes	**Figure 5-8 Subscriber Logout Window: Version 2**

Table 5-6 Subscriber Pop-up Logout Windows Variations

ACCOUNTING TYPE FIELD	RADIUS SERVER SESSION TIMEOUT MESSAGE	LOGOUT WINDOW EXAMPLE
Accumulation	No	**Logout Window** **You can use Internet now!** This is a logout window. Do not close this window before you want to logout. Connection Time: 0:0:9 If you don't want to continue to use Internet, please remember to logout. Otherwise, the login timer is still counting. Just click the following button. Logout **Figure 5-9 Subscriber Logout Window: Version 3**

5.2.7 Subscriber Manual Logout

When using the **Built-in Authentication** management type, there are two ways a subscriber manually logs out and terminates the Internet access for the **Accumulation** accounting method (refer to *Section 5.2.5* for more information).

➢ You can set the VSG to automatically display the logout screen after a successful login. Subscribers click on the **Logout** button in the logout screen to log out of the account.

➢ Or, the subscribers can manually log out by entering "http://1.1.1.1/Logout" in the web browser.

To display the Internet time usage information, enter "http://1.1.1.1/Time".

5.3 User Agreement Page

In cases where user authentication is not required and anyone can access the Internet through the VSG, you can set the VSG to redirect users to an Internet service usage agreement page. Users *must* accept the service usage agreement before they can access the Internet.

5.4 Subscriber Management Screen
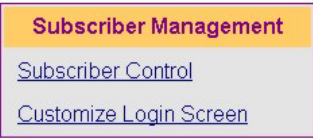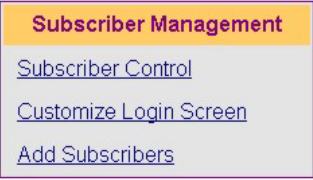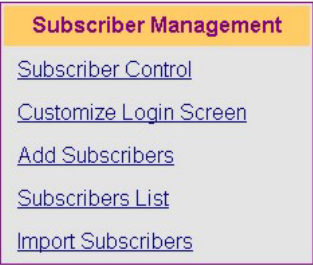
The **Subscriber Management** screen varies depending on the settings in the **Subscriber Control** screen.

The following table summarizes the different **Subscriber Management** screens and the configuration options in the **Subscriber Control** screen.

Table 5-7 Subscriber Management Main Menu Variations

SUBSCRIBER CONTROL SETTING	SUBSCRIBER MANAGEMENT SCREEN
Subscriber Control = Disable or User Agreement	**Subscriber Management** Subscriber Control **Figure 5-10 Subscriber Management: Default Initial**

Table 5-7 Subscriber Management Main Menu Variations

SUBSCRIBER CONTROL SETTING	SUBSCRIBER MANAGEMENT SCREEN
Subscriber Control = Enable Management Type = RADIUS	**Figure 5-11 Web Configurator: Subscriber Management: Version 2**
Subscriber Control = Enable Management Type = Built-in Authentication Billing Mechanism = Enable	**Figure 5-12 Web Configurator: Subscriber Management: Version 3**
Subscriber Control = Enable Management Type = Built-in Authentication Billing Mechanism = Disable	**Figure 5-13 Web Configurator: Subscriber Management: Version 4**

Chapter 6
Local Subscriber Management

This chapter shows you how to set up subscriber accounts on the VSG when using the Built-in Authentication management type.

6.1 Introduction

When you select the **Built-in Authentication** management type in the **Subscriber Control** screen, the subscriber account and/or accounting (or billing) information is stored in the VSG. You can store up to 250 subscriber accounts on the VSG.

From the **Main Menu** screen, click **Configuration**, **Subscriber Management** and **Add Subscribers**. The **Add Subscribers** screen varies depending on whether the billing mechanism is activated.

The Built-in Authentication **management type supports** Accumulation **accounting method only (refer to the *Accounting Method* section for more information).**

6.2 Subscriber Management without Billing

The following sections describe the local subscriber account management without the billing function.

Subscriber Management

Subscriber Control

Customize Login Screen

Add Subscribers

Subscribers List

Import Subscribers
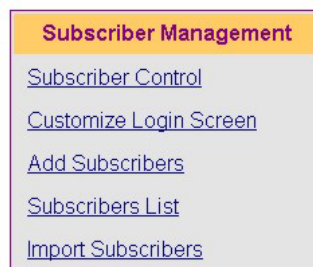
Figure 6-1 Subscriber Management Screen: No Billing

6.2.1   Editing Subscriber Account

Use the **Add Subscribers** screen to create and modify subscriber account information. You can create up to 10 subscriber accounts at a time.

Figure 6-2 Add Subscribers (No Billing)

The following table describes the labels in this screen.

Table 6-1 Add Subscribers (No Billing)

LABEL	DESCRIPTION
No	This read-only field displays the index number of the subscriber account.
Username	Enter the user name (up to 32 characters) for this account.
Password	Enter the password (up to 20 characters) in this field.
Apply	Click **Apply** to save the changes back to VSG and go back to the **Utility Menu**.
Clear	Click **Clear** to start configuring this screen again.
Home	Click **Home** to go back to the **Main Menu** screen. The changes you made will not be saved if you have not clicked **Apply**.
Previous	Click **Previous** to go back to the previous screen. The changes you made will not be saved if you have not clicked **Apply**.

6.2.2   Display Subscriber Account List

To display a list of subscriber accounts currently configured on the VSG, click **Subscribers List** in the **Subscriber Management** screen.

Click the **Username** or **Password** column headings to sort the entries.

Figure 6-3 Subscribers List (No Billing)

The following table describes the labels in this screen.

Table 6-2 Subscribers List (No Billing)

LABEL	DESCRIPTION
No	This read-only field displays the index number.
Username	This field displays the user name for an account.
Password	This field displays the password for the account.
Delete	Select the check box(es) and click **Delete** to remove the account(s) from the VSG.
Home	Click **Home** to go back to the **Main Menu** screen. The changes you made will not be saved if you have not clicked **Apply**.
Previous	Click **Previous** to go back to the previous screen. The changes you made will not be saved if you have not clicked **Apply**.

6.2.3   Importing Subscriber List

To generate a number of subscriber accounts automatically, import a subscriber list to the VSG via a TFTP server.

You must first create a text file with the user name and password pair in the format "username, password". Each line must contain only one account user name and password pair. The user name and password for each account must be separated with a comma. Spaces between the comma and the password are allowed. An example is shown in the following figure.

```
John, johng
Steve,     1234stevew
Phillip,phillips
```

Figure 6-4 Import Subscriber File Example

Follow the steps below to import a subscriber list to the VSG.

Step 1.   Create a subscriber list in a text file.

Step 2.   Run a TFTP server program and specify the location of the subscriber list file and the communication mode. Refer to the user's guide that comes with the TFTP server program for instructions.

Step 3.   Display the **Import Subscribers** screen as shown.

Figure 6-5 Import Subscribers (No Billing)

Step 4.   Enter the IP address of the computer running a TFTP server in the **TFTP Server IP Address** field.

Step 5.   Enter the name of the subscriber list file in the **Filename** field and click **Apply**.

Step 6.   After the subscriber list file is transferred to the VSG successfully, the **Subscriber Management** screen displays. Click **Subscriber List** to check the newly created subscriber accounts. The following figure shows the created accounts for the subscriber list file example in *Figure 6-4*.

Figure 6-6 Subscriber List (No Billing): Import Example

6.3 Subscriber Management with Billing

The following sections describe subscriber account management with simple billing feature. The VSG provides prepay and post-pay billing features.

With prepay billing, you set up how many time units a subscriber has purchased. The VSG automatically disconnects the subscriber after the time units are used up.

For post-pay billing, the VSG keeps track of how long a subscriber accesses the Internet until the subscriber logs out. You can then print out the billing information and send it to the subscriber.

Figure 6-7 Subscriber Management Screen: With Billing

6.3.1 Adding New Subscribers

Use the **Add New Subscribers** screen to create new subscriber accounts. You can only add one subscriber account at any one time.

Figure 6-8 Add New Subscribers

The following table describes the labels in this screen.

Table 6-3 Add New Subscribers (With Billing)

LABEL	DESCRIPTION
Username	Enter the user name (up to 32 characters) for this account.
Password	Enter the password (up to 20 characters) in this field.
Units	Enter the number of time units (either per day or per hour). Refer to the *Billing Mechanism* section for more information. Enter 0 for post-pay billing.
Create Account	Click **Create Account** to add a new subscriber account to the VSG.
Account Modify	Click **Account Modify** to make changes to the subscriber account information. Refer to *Section 6.3.2* for more information.
Account Information	Click **Account Information** to display a list of subscribers currently using the Internet through the VSG. Refer to *Section 6.3.3* for more information.
Home	Click **Home** to go back to the **Main Menu** screen. The changes you made will not be saved if you have not clicked **Apply**.
Previous	Click **Previous** to go back to the previous screen. The changes you made will not be saved if you have not clicked **Apply**.

6.3.2   Editing Subscriber Account Information

Use the **Account Modify** screen to monitor logged-in subscribers.

In the **Add New Subscriber** screen, click **Account Modify**. Click a column heading to sort the entries if applicable.

Figure 6-9 Add New Subscriber: Account Modify

Select the check box to edit an entry. The following table describes the labels in this screen.

Table 6-4 Add New Subscriber: Account Modify

LABEL	DESCRIPTION
Username	This field displays the user name for each account.
Login Time	This field displays the time the subscriber logged in to access the Internet. If a subscriber is not currently using the Internet through the VSG, this field is blank.

Table 6-4 Add New Subscriber: Account Modify

LABEL	DESCRIPTION
Expire Time	This field displays the time until which the subscriber can access the Internet. For prepay billing, this field is calculated by adding the number of time unit to the login time. For post-pay billing, this field is the time a subscriber logs out. If a subscriber is not currently using the Internet through the VSG, this field is blank.
Units	This field displays the number of time units (either per day or per hour) allocated to the subscriber account. Refer to the *Billing Mechanism* section for more information. Enter 0 for post-pay billing.
Display	Click **Display** to view detailed information on the selected subscriber account.
Delete	Click **Delete** once to disconnect the selected subscriber account from the VSG. An asterisk ("*") displays in the first column to indicate the subscriber account is terminated and prevented from logging into the VSG again. Click **Delete** twice to delete the selected subscriber account.
Apply	Click **Apply** to save the changes back to VSG and go back to the **Utility Menu**.
Clear	Click **Clear** to start configuring this screen again.
Home	Click **Home** to go back to the **Main Menu** screen. The changes you made will not be saved if you have not clicked **Apply**.
Previous	Click **Previous** to go back to the previous screen. The changes you made will not be saved if you have not clicked **Apply**.

6.3.3   Detailed Subscriber Accounting Information

To view detailed subscriber account information, click **Display** in the **Account Modify** screen.

Only one account's information is displayed at any one time. You can print out this screen for billing.

Account List					
Username	Password	Register Time	Login Time	Check out Time	Purchased Units
Cindy	2happy1	1982/10/19 09:57:26			10
Unit Price:	1	US			
Total	10.000000	US			

Back

Figure 6-10 Account Modify: Account List

The following table describes the labels in this screen.

Table 6-5 Account Modify: Account List

LABEL	DESCRIPTION
Username	This field displays the user name for an account.
Password	This field displays the password associated with the user name in the **Username** field.
Register Time	This field displays the time this account is created.
Login Time	This field displays the time a subscriber logs in. This field is empty if no subscriber logs in with this account.
Check out Time	This field displays the time a subscriber logs out. This field is empty if no subscriber logs in with this account.

Table 6-5 Account Modify: Account List

LABEL	DESCRIPTION
Purchase Units	This field displays the number of time units allocated to this account.
Unit Price	This field displays the cost of a time unit in the currency specified.
Total	This field displays the total price for the time units in the currency specified.
Back	Click **Back** to go back to the **Account Modify** screen.

6.3.4 Terminating or Deleting a Subscriber Account

To delete a subscriber account, click **Delete** in the selected account entry in the **Account Modify** screen. This removes the account entry immediately from the list.

To terminate a subscriber account that is currently in use, click **Delete** in the selected the account entry in the **Account Modify** screen. An asterisk displays to indicate that the account is being terminated. Once the account is not in use, click **Delete** again to remove the entry from the list.

If an account times out or has used up the allocated time, an asterisk displays to indicate that the account is being terminated. Click **Delete** to remove the entry from the list.

Figure 6-11 Account Modify: Terminating or Deleting a Subscriber Account

Part III:

Web Configurator Advanced Configuration

This part covers setting the login screen, port mapping, IP and MAC address pass through, wall garden and advertising links using the web configurator.

Chapter 7
Subscriber Login Screen

This chapter shows you how to customize the subscriber login screen when subscriber control is activated.

7.1 Overview

The subscriber login screen is the first screen that all subscribers see when trying to access the Internet. You can configure up to three web addresses for web sites which all subscribers are allowed to access without logging in. You must first activate subscriber control in the **Subscriber Management** screen.

Use the **Customize Login Screen** screen to configure the subscriber login screen. From the **Main Menu** screen, click **Configuration**, **Subscriber Management** and **Customize Login Screen**.

There are three ways in which you can customize the login screen: **Standard**, **Advanced** and **Frame**.

7.2 Standard Login Screen

The standard login screen is the VSG's pre-configured, default simple login screen. You can not change the standard login screen.

To set the VSG to display the standard login screen, select **Standard** in the **Selection** field.

Figure 7-1 Customize Login Screen: Standard

The following figure shows the default subscriber login screen.

Figure 7-2 Standard Subscriber Login Screen

7.3 Advanced Login Screen

Use the advanced login screen option to customize a login screen where you can create a welcome slogan and add advertising information. Select **Advanced** in the **Selection** field in the **Customize Login UI** screen.

Figure 7-3 Customize Login Screen: Advanced

The following table describes the labels in this screen.

Table 7-1 Customize Login Screen: Advanced

LABEL	DESCRIPTION
Selection	Select **Advanced** to configure and set the VSG to display the advanced subscriber login screen.
Welcome Image	Select **Default (Welcome!)** to display the default welcome image. Select **None** if you don't want to display the default welcome image.
Welcome Slogan	Enter a welcome message (up to 80 characters long) in the text box provided.
Page Background	Select **None** to set the background color of the login screen to white (the default). Select **Background Color** to set the color of the login screen background to the color specified, for example, enter '000000' for black. Click **View Color Grid** to display a list of web-friendly colors and corresponding hexadecimal values.
Article	Enter a block of text (up to 1024 characters long) in the text box. This is useful for advertisement or announcements.
Article Text Color	Select **None** to set the article text color of the login screen to white (the default). Select and set the color of the article text block background to the color specified, for example, enter '000000' for black. Click **View Color Grid** to display a list of web-friendly colors and corresponding hexadecimal values.
Information	Enter information such address and telephone or fax numbers in the text box provided. Up to 80 characters allowed.
Comments	Enter any comments (up to 80 characters long) in the text box provided.
Registration Prompt	Enter direction (up to 80 characters long) to tell the first-time users how to sign up for services online.

Table 7-1 Customize Login Screen: Advanced

LABEL	DESCRIPTION
Registration Text Color	Specify the color of the registration text. For example, enter '000000' for black. Click **View Color Grid** to display a list of web-friendly colors and corresponding hexadecimal values. The default is black ("000000").
Apply	Click **Apply** to save the changes back to VSG and go back to the **Utility Menu**.
Clear	Click **Clear** to start configuring this screen again.
Home	Click **Home** to go back to the **Main Menu** screen. The changes you made will not be saved if you have not clicked **Apply**.
Previous	Click **Previous** to go back to the previous screen. The changes you made will not be saved if you have not clicked **Apply**.

You can enter simple HTML tags such as <b> in the text box for formatting purposes.

The following figure shows an example of an advanced subscriber login screen.
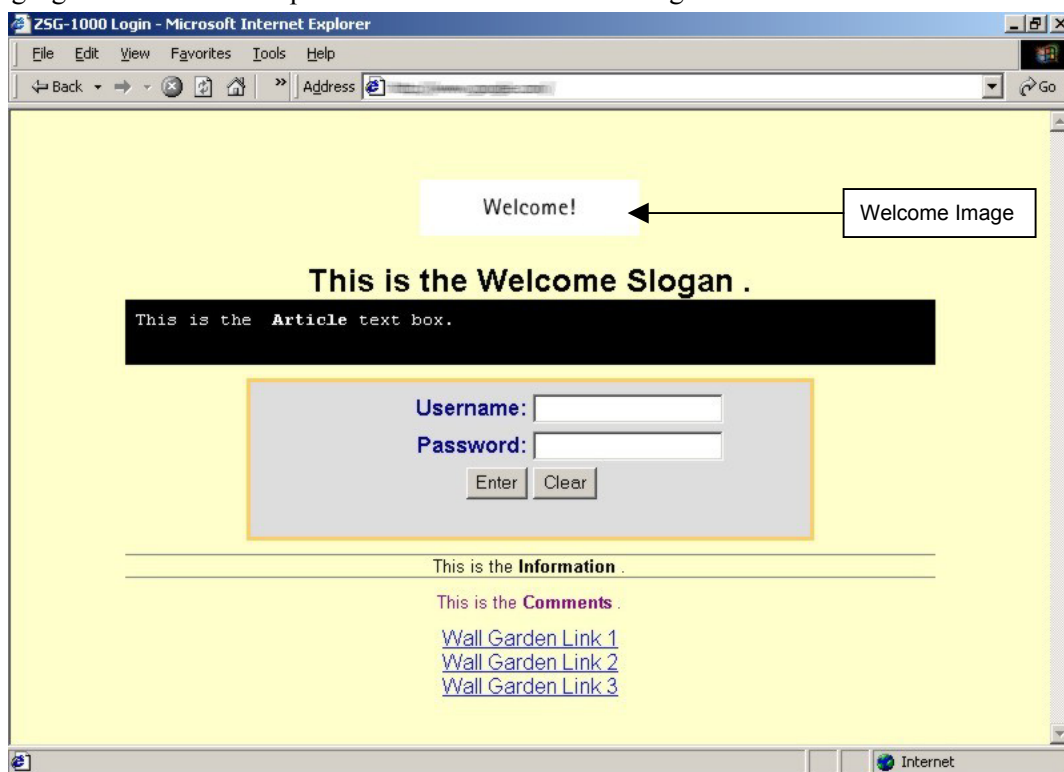
Figure 7-4 Advanced Subscriber Login Screen Example

Refer to the next chapter to configure wall garden and advertisement links.

7.4 Frame Login Screen

The frame login screen splits the login screen into two frames: top and bottom. You can specify a web site to be displayed in the top frame while the bottom frame contains the user name and password prompt. The frame login screen is useful for you to link to a web site (such as the company web site) as your welcome screen. In addition, you can externally design a web page with images and/or advanced multimedia features.

Select **Frame** in the **Selection** field in the **Customize Login UI** screen.

Figure 7-5 Customize Login Screen: Frame

The following table describes the fields in this screen.

Table 7-2 Customize Login Screen: Frame

FIELD	DESCRIPTION
Selection	Select **Frame** to configure and set the VSG to display the subscriber login screen in two frames.
Frame Setting	
Up Frame	Enter the IP address in decimal notation of a web server in the **web Server IP** field, for example, 192.168.1.1. Enter a web site address in the **URL Link** field, for example, http://www.zyxel.com.
Down Frame	Specify the color of the frame background. For example, enter '000000' for black. Click **View Color Grid** to display a list of web-friendly color and corresponding hexadecimal values. The default is black ("000000").
Apply	Click **Apply** to save the changes back to VSG and go back to the **Utility Menu**.
Clear	Click **Clear** to start configuring this screen again.
Home	Click **Home** to go back to the **Main Menu** screen. The changes you made will not be saved if you have not clicked **Apply**.
Previous	Click **Previous** to go back to the previous screen. The changes you made will not be saved if you have not clicked **Apply**.

The following figure displays a frame login screen example.
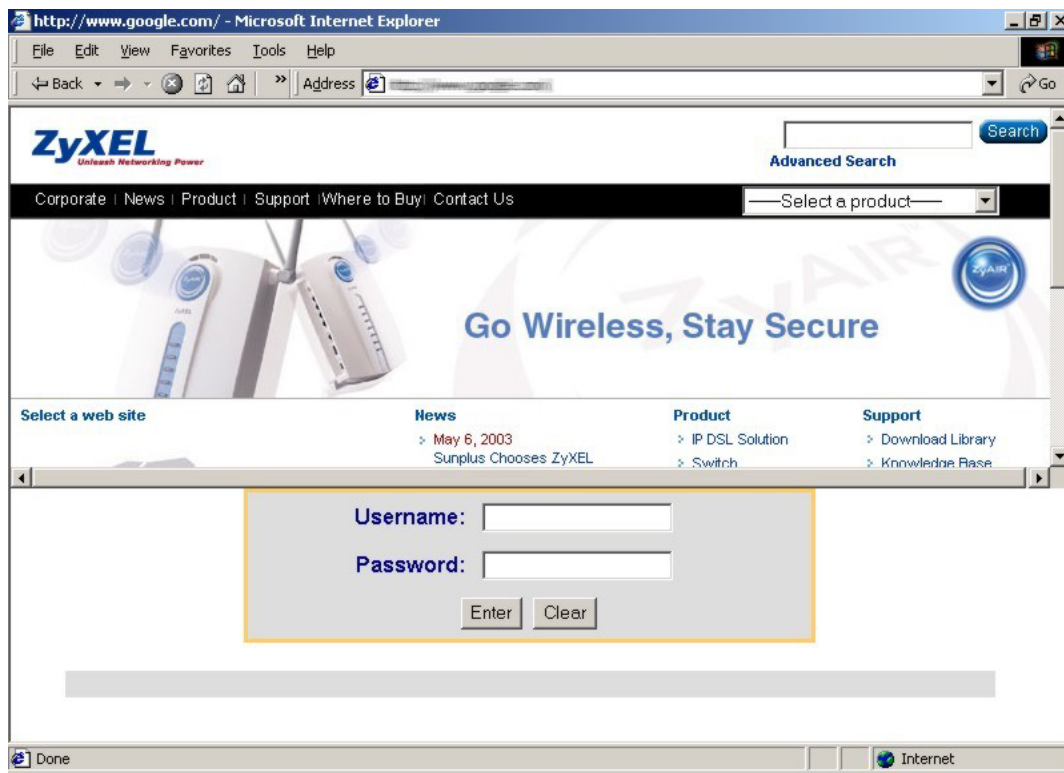
Figure 7-6 Frame Subscriber Login Screen Example

Refer to the next chapter to configure walled garden and advertisement links.

Chapter 8
Portal Web Site, Advertisement Link and Walled Garden

This chapter shows you how to specify a portal web site, advertisement links and create walled garden web sites.

8.1 Introduction

When you enable subscriber control in the **Subscriber Management** screen, you can set the VSG to direct a subscriber to a portal web site, display advertising web site pop-up window or activate the walled garden feature for generating on-line advertising revenues.

8.2 The Portal Page and Advertisement Links

You can set the VSG to direct a subscriber to a specified portal web site and/or display advertising web sites in a pop-up window after the subscriber logs in successfully. The advertising web site window pops up in random order. From the **Main Menu** screen, click **Configuration** and **Advertisement Link**.

Advertisement Link Configuration	
Portal Page	
Frequency	⊙ One Time Only ○ Every [0] minutes
URL Link 1	
URL Link 2	
URL Link 3	
URL Link 4	
URL Link 5	
URL Link 6	
URL Link 7	
URL Link 8	
URL Link 9	
URL Link 10	
Walled Garden	○ Enable ⊙ Disable

Apply   Clear

Home   **Previous**

Figure 8-1 Advertisement Link Configuration

The following table describes the labels in this screen.

Table 8-1 Advertisement Link Configuration

LABEL	DESCRIPTION
Portal Page	Specify the URL of a portal web site. This is the first web site to which a subscriber is directly after logging in successfully. If you do not specify a portal web site, the subscriber will be directed to the intended web site specified in the web browser.
Frequency	Select **One Time Only** to display an advertisement link in a pop-up browser window once after a subscriber logs in successfully.
	Select **Every ... minutes** to display an advertisement link in a pop-up window once every time period specified (in minutes) after a subscriber logs in successfully.
	The advertising web site window displays randomly one at a time.
URL Link 1 .. 10	Enter the web site addresses in the fields provided.
Walled Garden	Select **Enable** to activate this feature. Refer to *Section 8.3* for more information.
	Select **Disable** to de-activate this feature.
Apply	Click **Apply** to save the changes back to VSG and go back to the **Utility Menu**.
Clear	Click **Clear** to start configuring this screen again.
Home	Click **Home** to go back to the **Main Menu** screen. The changes you made will not be saved if you have not clicked **Apply**.
Previous	Click **Previous** to go back to the previous screen. The changes you made will not be saved if you have not clicked **Apply**.

8.3 Walled Garden

A subscriber must log in before the VSG allows the subscriber access to the Internet. However, with walled garden, you can define up to three web site addresses which all subscribers can access without logging in.

In the **Advertisement Link Configuration** screen, select **Enable** in the **Walled Garden** field.

Figure 8-2 Walled Garden

The following table describes the fields to configure the walled garden feature.

Table 8-2 Walled Garden

FIELD	DESCRIPTION
Walled Garden	Select **Enable** to activate this feature and set the field(s) below.
	Select **Disable** to de-activate this feature.
Link 1 … 3	In the **Prompt** field, enter a descriptive name (up to 80 characters) for the wall garden link to be displayed in the web browser.
	In the **Link Page** field, enter the web site address (up to 200 characters) of the web site.
	See *Figure 7-4* for a sample display in the login screen.

Chapter 9
LAN Device Management

This chapter describes how you can remotely manage devices on the LAN through the VSG.

9.1 LAN Device Management Overview

NAT (Network Address Translation - NAT, RFC 1631) is the translation of the IP address of a host in a packet. For example, the source address of an outgoing packet, used within one network is changed to a different IP address known within another network.

Traditionally, when you have a device (for example, a switch or a web server) on a LAN using NAT, you cannot access the device from the WAN since the LAN device is assigned a private IP address.

Your VSG is a NAT-enabled device that makes your whole inside network appear as a single computer to the outside world.

9.1.1 Port Mapping

To make LAN devices behind the VSG visible to the outside world, you configure a mapping between a virtual port on the VSG and a server port on a LAN device. A virtual port is a port on the VSG that appears as a physical port to the attached devices. A server port defines a server to which all specified requests are forwarded.

9.2 Configuring LAN Device Management

From the **Main Menu** screen, click **Configuration** and **LAN Device Management** to display the screen as shown below.

Figure 9-1 LAN Device Management

The following table describes the labels in this screen.

Table 9-1 LAN Device Management

LABEL	DESCRIPTION
No.	This read-only field displays the index number of an entry.

Table 9-1 LAN Device Management

LABEL	DESCRIPTION
IP Address	Enter the IP address of a LAN device in doted decimal notation. For example, 10.59.1.111.
Server Port	Enter the port number for a service (for example, 80 for HTTP) on the LAN device.
Virtual Port	Enter a unique port number between 9601 and 9650 to map to the port number in the **Server Port** field.
Application	Select an application type from the drop-down list box. Choose from **HTTP** (web), **FTP**, **Other TCP** or **Other UDP**. Only requests for the selected application type are forwarded to the specified server port on the LAN device.
MAC Address	Enter the MAC address of the LAN device in hexadecimal notation in 6 hexadecimal pairs, for example, 00-50-BA-8D-22-96. Make sure you enter the correct MAC address.
Apply	Click **Apply** to save the changes back to VSG and go back to the **Utility Menu**.
Clear	Click **Clear** to start configuring this screen again.
Home	Click **Home** to go back to the **Main Menu** screen. The changes you made will not be saved if you have not clicked **Apply**.
Previous	Click **Previous** to go back to the previous screen. The changes you made will not be saved if you have not clicked **Apply**.

9.2.1 LAN Device Management Example

In this example, there is a manageable switch behind the VSG and you want to be able to remotely access the web-based management interface on the manageable switch over the Internet.
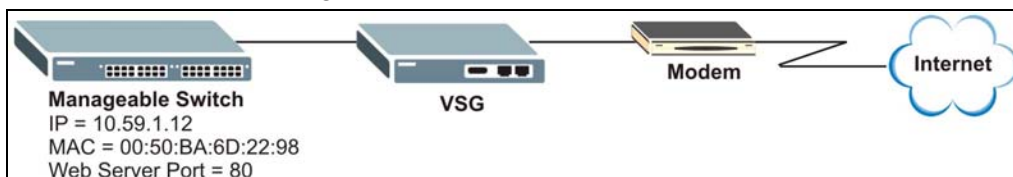
Figure 9-2 Configuring for LAN Device Remote Management

You map virtual port 9603 on the VSG to the web server port on the manageable switch.

Figure 9-3 LAN Device Management: Remote Management Example

To access the web-based management interface, enter the WAN IP address of your VSG and the virtual port number of the LAN device separated by a colon. In this example, enter "http:// 172.168.1.1:9601" where 172.168.1.1 is the WAN IP address of the VSG.

9.2.2 Specifying an Inside Server Example

Let's say you have a web server behind the VSG as shown in the next figure.
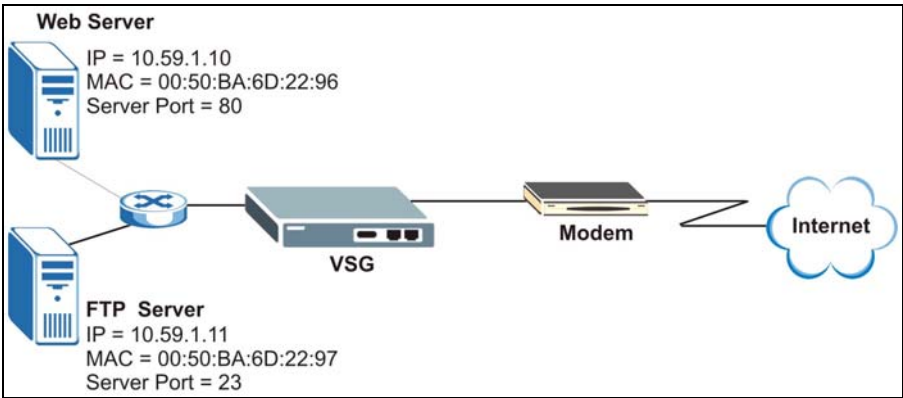
Figure 9-4 Specifying an Inside Server Example

In the **LAN Device Management** screen, you map virtual port 9601 to the web server and virtual port 9602 to the FTP server.

No.	IP Address	Server Port	Virtual Port (9601~9650)	Application	MAC Address
1	10.59.1.10	80	9601	HTTP	10-50-BA-6D-22-96
2	10.59.1.11	23	9602	FTP	10-50-BA-6D-22-97
3		0	0	HTTP	
4		0	0	HTTP	

Figure 9-5 LAN Device Management: Inside Server Example

To access an inside server on the LAN, enter the WAN IP address of your VSG and the virtual port number of the inside server separated by a colon. In this example, to access the FTP server, enter "http:// 172.168.1.1:9602" where 172.168.1.1 is the WAN IP address of the VSG.

You can also access the server by entering the domain name provided that you specified a DNS server on the VSG. Enter the domain name and the virtual port number separated by a colon, for example, http://www.domainName:9602.

Chapter 10
IP and MAC Address Pass Through

This chapter shows you how to configure IP and MAC address pass through.

10.1 Configuring IP and MAC Address Pass Through

You can set the VSG to allow the forwarding of packets from a specified LAN device, such as a file server or computer, without prompting for a user name and password. You can specify up to 40 IP addresses and 10 MAC addresses of LAN devices allowed to pass through the VSG. For example, in an airport VIP room, you can specify the IP or MAC addresses of computers that subscribers can use without logging in.

From the **Main Menu** screen, click **Configure**, **Pass Through IP & MAC**. A screen displays as shown.

Figure 10-1 IP & MAC Address Pass Through

The following table describes the labels in this screen.

Table 10-1 IP & MAC Address Pass Through

LABEL	DESCRIPTION
No.	This read-only field displays the index number of the entry.
IP Address	Enter the IP address of the device (in dotted decimal notation) whose packets are allowed to pass through the VSG. For example, 10.59.1.10.
MAC Address	Enter the MAC address of the device (in 6 hexadecimal pairs, for example, 00-50-BA-8D-22-96) whose packets are allowed to pass through the VSG.
Apply	Click **Apply** to save the changes back to VSG and go back to the **Utility Menu**.
Clear	Click **Clear** to start configuring this screen again.
Home	Click **Home** to go back to the **Main Menu** screen. The changes you made will not be saved if you have not clicked **Apply**.

Table 10-1 IP & MAC Address Pass Through

LABEL	DESCRIPTION
Previous	Click **Previous** to go back to the previous screen. The changes you made will not be saved if you have not clicked **Apply**.

Chapter 11
Status

This chapter covers the system status, DHCP client and current logged-in subscriber information.

11.1 System Status

In the **Main Menu**, click **Status** and **System** to display the system information as shown next.

System Status	
System Name	VSG-1000
Console Port Speed	9600 bps
Date	2004/08/20
Time	15:05:34
WAN	
MAC Address	00-A0-C5-41-D0-53
WAN Mode	DHCP Client
IP Address	172.21.3.188
Subnet Mask	255.255.0.0
Default Gateway	172.21.0.254
Web Server Port	80
DHCP	
Status	Disabled
Server IP Address	N/A
E-Mail Server IP Address	N/A
DNS	
Primary IP Address	172.20.0.63
Secondary IP Address	172.20.0.27

Home   **Previous**

Figure 11-1 System Status

The following table describes the labels in this screen.

Table 11-1 System Status

LABEL	DESCRIPTION
System Name	This field displays the description name of the VSG for identification purposes.
Consol Port Speed	This field displays the speed of the console port on the VSG.
Date	This field displays the current date in yyyy/mm/dd format.
Time	This field displays the current time in hh:mm:ss 24-hour format.
WAN	
MAC Address	This field displays the MAC address of the WAN port on the VSG.
WAN Mode	This field displays the DHCP mode of the WAN port. It displays either **DHCP Client** or **Static IP Setting**.
IP Address	This field displays the IP address of the WAN port on the VSG.
Subnet Mask	This field displays the subnet mask of the WAN port on the VSG.

Table 11-1 System Status

LABEL	DESCRIPTION
Default Gateway	This field displays the IP address of the default gateway of the WAN port on the VSG.
Web Server Port	This field displays the port number of the embedded web server in your VSG.
DHCP The following fields display the status of the DHCP status on the LAN port of the VSG.	
Status	This field displays DHCP setting (**Server**, **Client** or **Relay**) of the VSG.
Server IP Address	This field displays the LAN IP address of the VSG.
Start IP Address	This field displays the first of the contiguous addresses in the client IP address pool.
End IP Address	This field displays the last of the contiguous addresses in the client IP address pool.
Subnet Mask	This field displays the LAN subnet mask.
Lease Time	This field displays the lease time of the IP addresses to the DHCP clients.
E-mail Server Address	The field displays the IP address or the domain name of the SMTP server.
DNS	
Primary IP Address	This field displays the IP address of the primary DNS server.
Secondary IP Address	This field displays the IP address of the secondary DNS server.
Home	Click **Home** to go back to the **Main Menu** screen. The changes you made will not be saved if you have not clicked **Apply**.
Previous	Click **Previous** to go back to the previous screen. The changes you made will not be saved if you have not clicked **Apply**.

11.2 DHCP Client Table

In the **Main Menu**, click **Status** and **DHCP Client Table**.

The DHCP table shows current DHCP client information of all network clients using the DHCP server on the VSG.

DHCP Client Table	
IP Address	MAC Address
10.59.1.2	00-50-ba-ad-4f-81
Home	**Previous**

Figure 11-2 DHCP Client Table

The following table describes the labels in this screen.

Table 11-2 DHCP Client Table

LABEL	DESCRIPTION
IP Address	This field displays the IP address assigned to the client computer.
MAC Address	This field displays the MAC address of the client computer. The MAC (Media Access Control) or Ethernet address on a LAN (Local Area Network) is unique to your computer (six pairs of hexadecimal characters). A network interface card such as an Ethernet adapter has a hardwired address that is assigned at the factory. This address follows an industry standard that ensures no other adapter has a similar address.
Home	Click **Home** to go back to the **Main Menu** screen. The changes you made will not be saved if you have not clicked **Apply**.

LABEL	DESCRIPTION
Previous	Click **Previous** to go back to the previous screen. The changes you made will not be saved if you have not clicked **Apply**.

11.3 Current Users

The **Current Users** screen displays a list of subscribers currently logged on to the VSG for Internet access.

This screen is available if you select RADIUS **subscriber management type or disable accounting (or billing) function in the** Subscriber Control **screen.**

From the **Main Menu** screen, click **Status** and **Current Users**. A screen displays as shown. Click a column heading to sort the entries if applicable.

No	Username	IP Address	MAC Address	Disconnect
1	Cindy	10.59.1.2	00-50-BA-AD-4F-81	Apply

Home   Previous

Figure 11-3 Web Configurator: Status: Current User

The following table describes the labels in this screen.

Table 11-3 Web Configurator: Status: Current User

LABEL	DESCRIPTION
No	This field displays the index number of the entry.
Username	This field displays the user name of an account.
Password	This field displays the password of an account.
MAC Address	This field displays the MAC address of the computer that is logged in using the account.
Disconnect	Click **Apply** to terminate the connection to the selected subscriber.
Home	Click **Home** to go back to the **Main Menu** screen. The changes you made will not be saved if you have not clicked **Apply**.
Previous	Click **Previous** to go back to the previous screen. The changes you made will not be saved if you have not clicked **Apply**.

Part IV:

The SMT, System Maintenance and Additional Information

This part contains information on the SMT (System Management Terminal), configuration and firmware maintenance, troubleshooting, appendices and an index.

Chapter 12
The SMT

This chapter introduces the operation of the SMT.

12.1 Introduction to the SMT

The System Management Terminal (SMT) is a menu – driven interface that you use to configure the VSG. Access the SMT using the console port.

Use the SMT to set general system settings and upgrade firmware. For advanced configuration, use the embedded web configurator (refer to the chapters on web configuration).

12.1.1   Establishing a Console Port Connection

After the VSG is directly connected to a computer using the console port, turn on the computer and run a terminal emulation program (for example, Hyper Terminal in Windows) and configure its communication parameters as follows:

➢ 9600 bits per second.
➢ Parity none, 8 data bits, 1 stop bit, flow-control none.
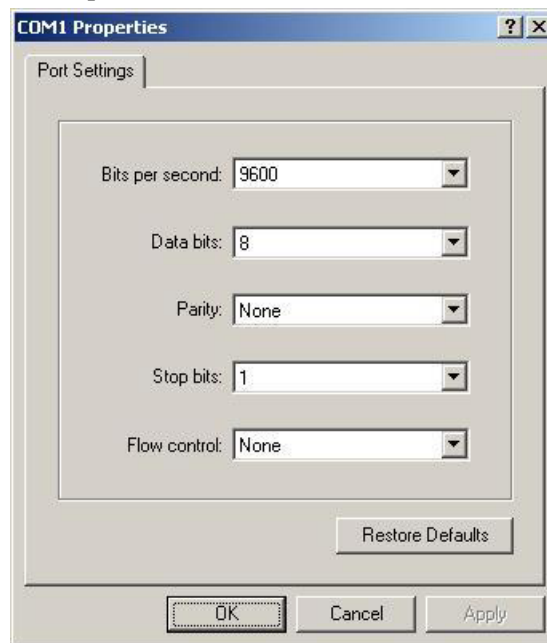
Figure 12-1 HyperTerminal Communication Parameter Settings Example

12.2 SMT Login Screen

Press [ENTER] to display the login screen. For your first login, enter the default user name "admin" and default password "1234" and then press [ENTER].

The user name and password are case sensitive.

```
                              VSG-1000

        (c) 2000-2003 ZyXEL Communications Corporation. All Rights Reserved.

                            Version 1.06


                       Username:

                       Password:
```
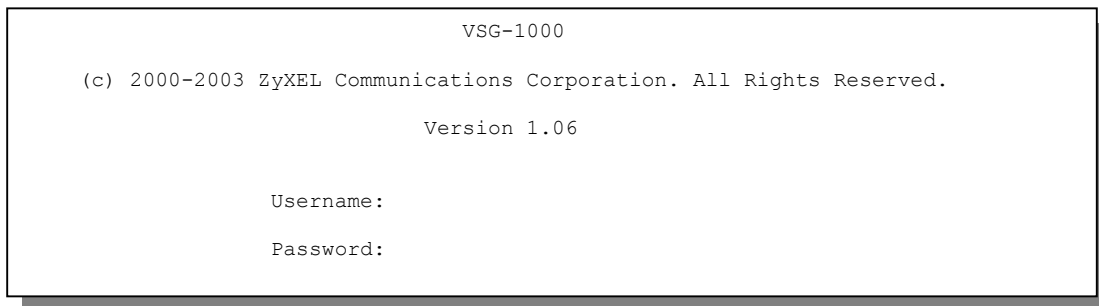
Figure 12-2 SMT: Login Screen

The VSG automatically logs you out after ten (default) minutes of inactivity. Simply log back into the VSG if this happens to you.

12.3 The SMT Main Menu Summary

The SMT main menu is shown next.

```
                            Main Menu


              1)System Configuration
              2)Status
              3)Utilities
              4)Restart
              5)Logout
              6)Factory Setting


              Enter selection:

Enter a numeric between 1-6.
```
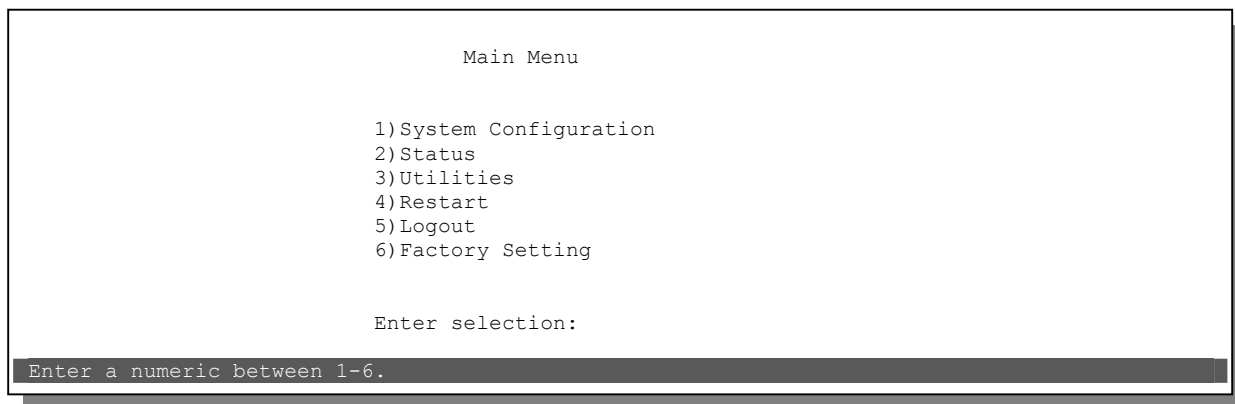
Figure 12-3 SMT: Main Menu

The following table describes the menu choices in this screen.

NUMBER	MENU TITLE	FUNCTION
1	System Configuration	Use this menu to set up LAN IP address, DHCP settings, WAN port configuration and general system setup.
2	Status	Use this menu to view the current configuration of the VSG.
3	Utilities	Use this menu to perform firmware upgrade and change login password.
4	Restart	Use this menu to restart your VSG.
5	Logout	Use this menu to log out of the SMT.
6	Factory Setting	Use this menu to reset the VSG back to factory default settings.

12.4 Navigating the SMT Interface

Familiarize yourself with the SMT operations before you attempt to modify the configuration.

12.4.1   SMT Screen Breakdown

The following figure shows the breakdown of most SMT screens.
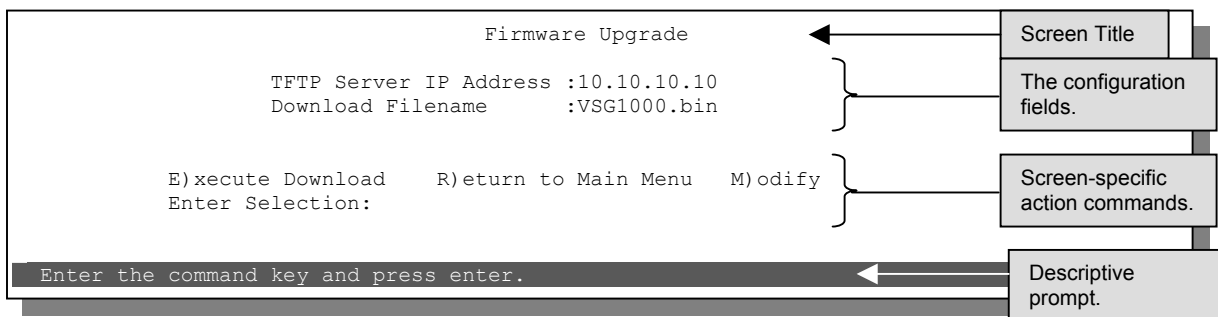
Figure 12-4 SMT: Menu Breakdown

12.4.2   The Navigation Keys

The following table describes the keystrokes that you use in the SMT screens.

Table 12-1 Control Key Descriptions

KEY	DESCRIPTION
[ENTER]	To move to the next configuration field in the menu.
[ESC]	Press [ESC] to discard any changes and return to the previous screen.

Chapter 13
System Configuration Using the SMT

This chapter shows you how to set general system settings, view current configuration and perform system maintenance.

13.1 About SMT System Configuration

Refer to the *System Configuration* chapter for background information.

13.2 Setting System Configuration

From the main menu, type 1 and press [ENTER] to display the **System Configuration** menu.

```
                     System Configuration
  SystemName             :VSG-1000
  Console Port Speed      :9600
  Auto Logout Timer       :10
  WAN Configuration
      WAN Mode? (D/S)     :S
      IP Address          :192.168.1.1
      Subnet Mask         :255.255.255.0
      Gateway             :192.168.1.254
      Web Server Port     :80
  DHCP Configuration
      DHCP Service? (D/R/S) :S
      Server IP Address   :10.59.1.1
      Start IP Address    :10.59.1.2
      End IP Address      :10.59.1.253
      Subnet Mask         :255.255.255.0
      Lease Time          :300
  E-Mail Server IP Address  :
  Primary DNS IP Address    :168.95.1.1
  Secondary DNS IP Address  :


   Enter WAN IP address
```

Figure 13-1 SMT: System Configuration

The following table describes the fields in this screen.

Table 13-1 SMT: System Configuration

FIELD	DESCRIPTION
System Name	Enter a descriptive name for identification purposes.
Console Port Speed	Enter **9600**, **19200** or **38400** to set the console port speed. The default setting is **9600**.
	If you change the console port speed, make sure you also make the same change to the terminal emulator software.
Auto Logout Timer	Specify how many minutes (between 0 and 60) the SMT session can be left idle before the session times out. The default is 10 minutes. After it times out you have to log in with your password again. Very long idle timeouts may have security risks.
	A value of "0" means a management session never times out, no matter how long it has been left idle (not recommended).
	This does *not* apply to the web configurator.

Table 13-1 SMT: System Configuration

FIELD	DESCRIPTION
WAN Configuration Set the following fields for the **WAN** port on the VSG.	
WAN Mode? (D/S)	Enter **D** (Dynamic) to set the VSG to dynamically obtain an IP address and other network information (IP address, DNS information etc.) from a DHCP server on the WAN network. Enter **S** (Static) to set the VSG to use a static (or fixed) IP address and assign network information (IP address, DNS information etc.) to Ethernet device(s) connected to the **WAN** port. This is the default setting. Then set the following fields.
IP Address	This field is available when you select **S** in the **WAN Mode** field. Enter the static IP address assigned to you by your ISP or network administrator. The default is **192.168.1.1**.
Subnet Mask	This field is available when you select **D** in the **WAN Mode** field. Enter the subnet mask depending on your network needs. The default is **255.255.255.0**. Refer to the *Subnetting* appendix if you are implementing subnetting.
Default Gateway	Enter the IP address of the default gateway.
Web Server Port	Specify the port number of the embedded web server on the VSG to access the web configurator. The default port number is **80**. Enter a number between 8000 and 8099 to access the web configurator behind a NAT-enabled network. If you enter a number between 8000 and 8099, you need to append the port number to the **WAN** port IP address to access the web configurator. For example, if you enter "8000" as the web server port number, then you must enter "http://www.192.168.1.1:8000" where 192.168.1.1 is the WAN port IP address.
DHCP Configuration Set the following fields for the **LAN** port on the VSG.	
DHCP Service? (D/R/S)	Enter **D** (Disable) to set the VSG to automatically obtain an IP address and other network information (DNS information etc.) from a DHCP server on the LAN network. Enter **R** (Relay) to set the VSG to forward network configuration requests to a DHCP server on the LAN network. Then configure the **Server IP Address** and **Agent IP Address** fields. Enter **S** (Server) to set the VSG to use a static (or fixed) IP address and assign network information (IP address, DNS information etc.) to Ethernet device(s) connected to the **LAN** port. Then configure the following fields.
Server IP Address	This field is visible when you enter **R** or **S** in the **DHCP Service** field. If the VSG is set to function as a DHCP relay, enter the IP address of the DHCP server. If the VSG is set to function as a DHCP server, then enter the LAN IP address of the VSG. **10.59.1.1** is the default.
Agent IP Address	This field is visible when you enter **R** in the **DHCP Service** field. Enter the IP address of the DHCP relay device. Usually this is the WAN IP address of the VSG.
Start IP Address	This field is visible when you enter **S** in the **DHCP Service** field. Enter the first of the continuous addresses in the IP address pool.
End IP Address	This field is visible when you enter **S** in the **DHCP Service** field. Enter the last of the continuous addresses in the IP address pool.
Subnet Mask	Enter the subnet mask based on the IP address you specified in the **DHCP Server IP Address**, **Start IP Address** and **End IP Address** fields. **255.255.255.0** is the default. Refer to the *Subnetting* appendix if you are implementing subnetting.
Lease Time	Specify the time (in minutes between 1 and 71582788) a DHCP client is allowed to use an assigned IP address. When the lease time expires, the DHCP client is given a new, unused IP address.
E-mail Server IP Address	Enter the IP address of the e-mail server to which the VSG forwards e-mail. This field should be configured if the e-mail server is behind a firewall or on a NAT-enabled network.

Table 13-1 SMT: System Configuration

FIELD	DESCRIPTION
Primary/Secondary DNS IP Address	Enter the IP address of the DNS server(s) in the **Primary DNS IP Address** and/or **Secondary DNS IP Address** fields.
	The default primary DNS server IP address is **168.95.1.1**.
	You *must* specify a DNS server.
At the "S)ave and return R)eturn without saving M)odify:" prompt, type **S** and press [ENTER] to save the changes and return to the previous screen, type **R** and press [ENTER] to discard all changes and return to the previous screen or type **M** and press [ENTER] to continue configuring the fields. Restart the device when prompted	
Press [ESC], **Y** and [ENTER] to stop any actions in the current screen and return to the previous screen. All changes will be discarded.	

13.3 View Current Configuration

From the main menu, enter 2 and press [ENTER] to display the **System Status** screen. If the VSG is set to dynamically obtain an IP address on the WAN port, use this screen to view the IP address.

```
                         System Status
 SystemName              :VSG-1000
 Console Port Speed      :9600
 Auto Logout Timer       :0
 WAN Configuration
      WAN Mode? (D/S)       :Static IP Setting
      IP Address            :192.168.1.1
      Subnet Mask           :255.255.255.0
      Gateway               :192.168.1.254
      Web Server Port       :80
 DHCP Configuration
      DHCP Service? (D/R/S) :Server
      Server IP Address     :10.59.1.1
      Start IP Address      :10.59.1.2
      End IP Address        :10.59.1.253
      Subnet Mask           :255.255.255.0
      Lease Time            :12345667
 E-Mail Server IP Address  :N/A
 Primary DNS IP Address    :168.95.1.1
 Secondary DNS IP Address  :N/A


 Press any key to return.
```

Figure 13-2 SMT: System Status

The following table describes the fields in this screen.

Table 13-2 SMT: System Status

FIELD	DESCRIPTION
System Name	This field displays the name of the VSG for identification purposes.
Console Port Speed	This field displays the consol port speed (**9600**, **19200** or **38400**).
Auto Logout Timer	This field displays how many minutes (0 to 60) the SMT session can be left idle before the session times out. The default is 10 minutes. After it times out you have to log in with your password again. Very long idle timeouts may have security risks.
	A value of "0" means a management session never times out, no matter how long it has been left idle (not recommended).
	This does *not* apply to the web configurator.
WAN Configuration	

Table 13-2 SMT: System Status

FIELD	DESCRIPTION
WAN Mode? (D/S)	This field displays the WAN IP address assignment method (**Static IP Setting** or **DHCP Client**).
IP Address	This field displays the WAN IP address of the VSG.
Subnet Mask	This field displays the subnet mask on the WAN port.
Default Gateway	This field displays the IP address of the default gateway.
Web Server Port	This field displays the port number for the embedded web server.
	If the port number is not **80**, then you need to append the port number to the **WAN** port IP address to access the VSG web configurator. For example, if 8000 is the web server port number, then you must enter "http://www.192.168.1.1:8000" in the address bar on the web browser where 192.168.1.1 is the WAN port IP address.
DHCP Configuration	
DHCP Service? (D/R/S)	This field displays the DHCP mode (**Server**, **Relay** or **Disable**) on the LAN port.
Server IP Address	This field is visible when the **DHCP Service** field displays **Server** or **Relay**.
	This field displays the IP address of the DHCP server.
Agent IP Address	This field is visible when the **DHCP Service** field displays **Relay**.
	This field displays the IP address of the DHCP relay agent.
Start IP Address	This field is visible when the **DHCP Service** field is **Server**.
	This field displays the first of the contiguous addresses in the IP address pool.
End IP Address	This field is visible when the **DHCP Service** field is **Server**.
	This field displays the last of the contiguous addresses in the IP address pool.
Subnet Mask	This field displays the subnet mask.
Lease Time	This field displays for how many minutes a DHCP client is allowed to use an assigned IP address.
Email Server IP Address	This field displays the IP address of the E-mail server to which the VSG forwards the e-mail.
Primary/Secondary DNS IP Address	These two fields display the IP address(es) of the DNS server(s).
Press any key at the "Press any to return" prompt to go back to the previous screen.	

13.4 Changing the System Password

It is recommended you change the default system password.

Follow the steps below to change the system password.

Step 1. In the main menu, type 3 and press [ENTER] to display the **Utilities** menu.

Step 2. In the **Utilities** menu, type 2 and press [ENTER]. The **Change Administrator Password** menu displays.

```
                    Change Administrator Password


          Enter the old password  :

          Enter the new password  :

          Confirm the new password:




  Enter the old password.
```

Figure 13-3 SMT: Change Administrator Password

Step 3. Type your current system password in the **Enter the old password** field, and press [ENTER].

Step 4. Type your new system password in the **Enter the new password** field, and press [ENTER].

Step 5. Re-type your new system password in the **Confirm the new password** field for confirmation and press [ENTER].

Step 6. Save the settings.

Note that as you type a password, the screen displays an asterisk "*" for each character you type.

13.5 Restarting the VSG

Follow the steps below to restart the VSG.

Step 1. In the main menu, type 4 and press [ENTER]. A screen displays prompting you to confirm.

```
                    Restart System (Y/N)?




  Enter the command key and press enter.
```

Figure 13-4 SMT: Restart

Step 2. Type **Y** and press [ENTER] to restart the VSG. Otherwise, type **N** and press [ENTER] to cancel the action and return to the main menu.

13.6 Reset the VSG to Factory Defaults

If you forgot your login user name and password, you have to reset the VSG back to factory defaults.

Resetting the VSG restores all system configuration back to factory defaults. However, you may retain the subscriber account information.

All system settings will be lost once you reset to the default settings.

Follow the steps below to reset the VSG back to factory defaults.

Step 1. In the main menu, type 6 and press [ENTER]. A screen displays prompting you to confirm.

Step 2. Type **Y** and press [ENTER] to reset the VSG.

Step 3. Type **Y** and press [ENTER] to retain the subscriber account information in the local subscriber database. Type **N** and press [ENTER] to delete all subscriber account information.

Step 4. Press [ENTER] to reset the VSG. The VSG automatically restarts.

```
                Are you sure you want to reset the device
                   back to the factory defaults? [Y/N]:




 Enter the command key and press enter.
```
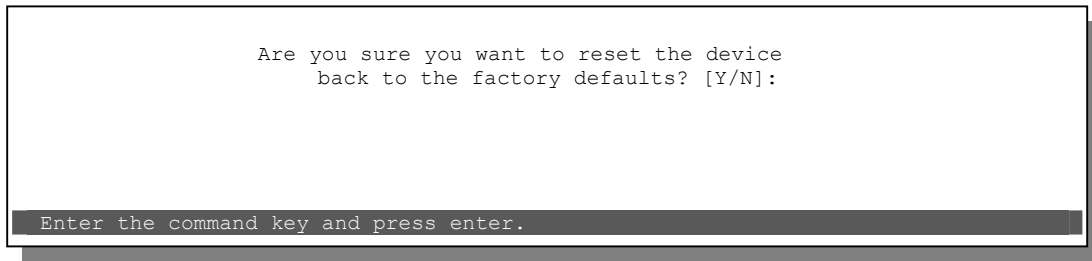
Figure 13-5 SMT: Reset to Factory Defaults

Chapter 14
Configuration and Firmware Maintenance

This chapter shows you how to upgrade the firmware and configuration file and create configuration backup files.

14.1 Configuration and Firmware Maintenance Overview

You need to run a TFTP server on a computer where the firmware and/or configuration files are stored to perform file upload or download. Use either the web configurator for file upload and download. You can configure the TFTP settings in the SMT but you *must* still have a WAN connection between the VSG and the TFTP server computer at the same time.

WARNING!
Do not interrupt the file upload process as this may PERMANENTLY damage the device.

14.2 Filename Convention

The firmware or the configuration files do not have any filename conventions. There is not a specific file extension or filenames conventions that you need to follow. Therefore, you can specify any name or file extension for the firmware and the configuration files.

However, it is recommended to use the ".bin" file extension for the firmware file and ".rom" for the configuration file for management purposes.

Visit www.zyxel.com to download the latest version of firmware for your VSG.

14.3 Firmware Upgrade

The following sections show you how to upgrade the firmware.

14.3.1   Firmware Upgrade Using SMT
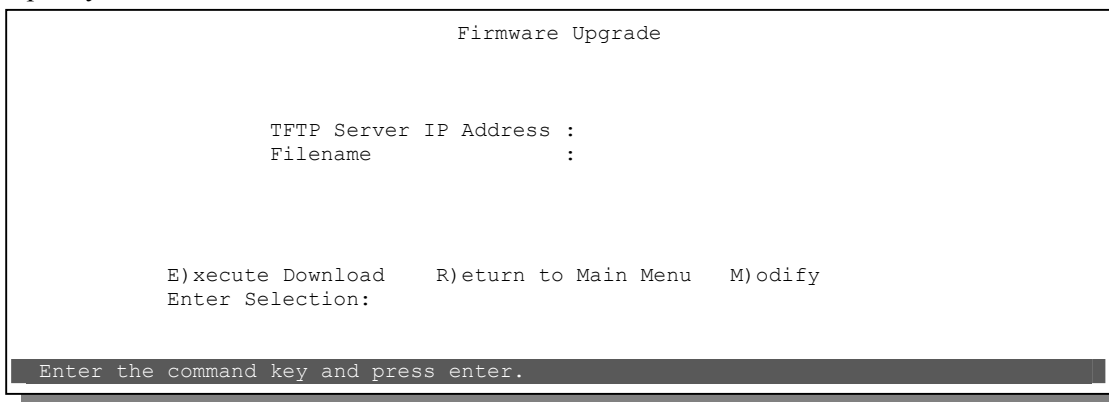
Follow the steps below to prepare for firmware upload using the SMT.

Step 1.   Run a TFTP server program and specify the location of the firmware file and the communication mode. Refer to the TFTP server program user's guide for instructions.

Step 2.   Connect the computer directly to the VSG through the console port and the WAN port. Refer to the section on establishing port connections for more information.

Step 3.   In the SMT main menu, type 3 and press [ENTER] to display the **Utilities Menu** screen.

```
                            Utilities Menu


                   1)Firmware Upgrade
                   2)Change Password
                   3)Return to Main Menu




                      Enter selection:
    Enter a numeric between 1-3.
```
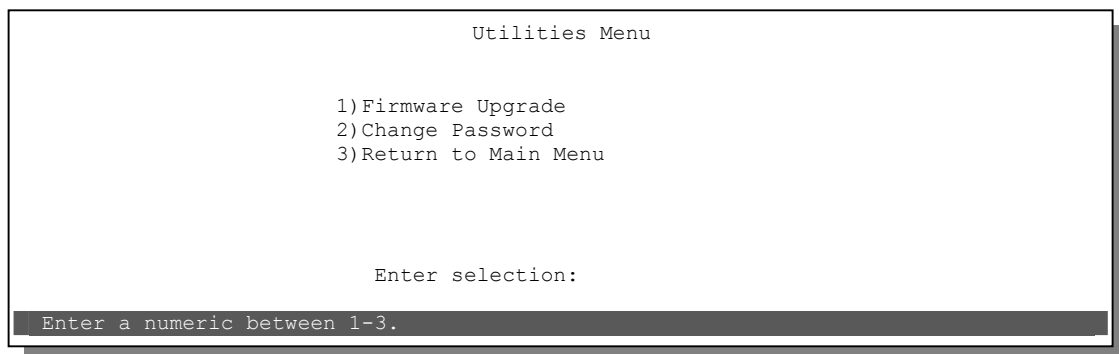
Figure 14-1 SMT: Utilities Menu

Step 4. Type 1 and press [ENTER] to display the **Firmware Upgrade** screen.

Step 5. Enter the IP address of the computer running the TFTP server in the **TFTP Server IP Address** field.

Step 6. Specify the name of the firmware file in the **Download Filename** field.

```
                            Firmware Upgrade



                 TFTP Server IP Address :
                 Filename               :




           E)xecute Download    R)eturn to Main Menu   M)odify
           Enter Selection:


   Enter the command key and press enter.
```

Figure 14-2 SMT: Firmware Upgrade

Step 7. Type **E** at the "Enter Selection:" prompt to get the firmware file from the TFTP server. You may type **A** to abort the firmware transfer at this point.

```
                 TFTP Server IP Address :10.10.10.10
                 Filename               :VSG1000.bin



           |---------+---------+---------+---------+---------|
           **************************************************

 A)bort Download:

                        Press 'A' to break download.
```

Figure 14-3 SMT: Firmware Upgrade Process 1

Step 8. The following message displays when the firmware is transferred successfully to the VSG. The VSG automatically restarts after the firmware upgrade is complete. Check the firmware version in the login screen.

```
              Saving the downloaded image file....

                   Saving data. Please wait...
```

Figure 14-4 SMT: Successful Firmware File Transfer

14.3.2   Firmware Upgrade Using the Web Configurator
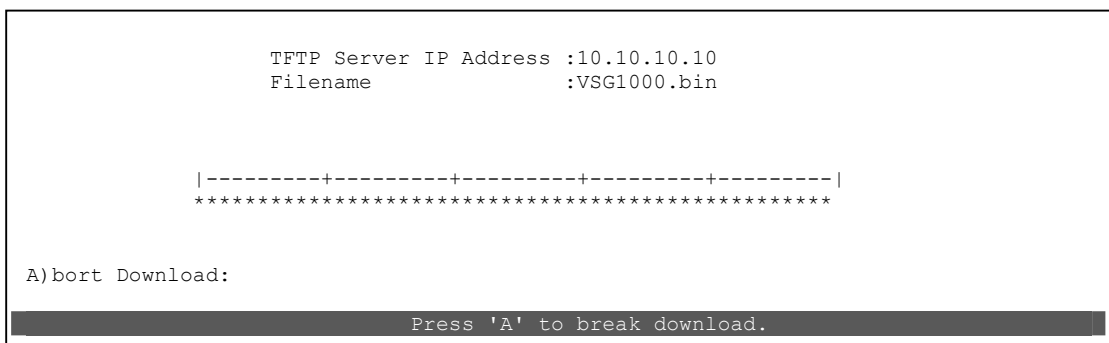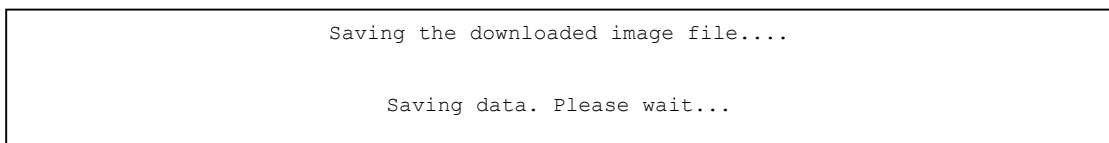
Follow the steps below to upload the firmware using the web configurator.

Step 1. Run a TFTP server program and specify the location of the firmware file and the communication mode. Refer to the TFTP server program user's guide for instructions.

Step 2. Access the web configurator. Refer to the section on accessing the web configurator for instructions.

Step 3. In the **Main Menu** screen, click **Utilities** and **Firmware Upgrade** to display the screen as shown.

Figure 14-5 Web Configurator: Firmware Upgrade

Step 4. Enter the IP address of the computer running the TFTP server in the **TFTP Server IP Address** field.

Step 5. Specify the name of the firmware file in the **Filename** field and click **Apply** to start the file transfer process.

Step 6. When the file transfer is completed successfully, a " TFTP Downloading 100%" message displays and the VSG automatically restarts.
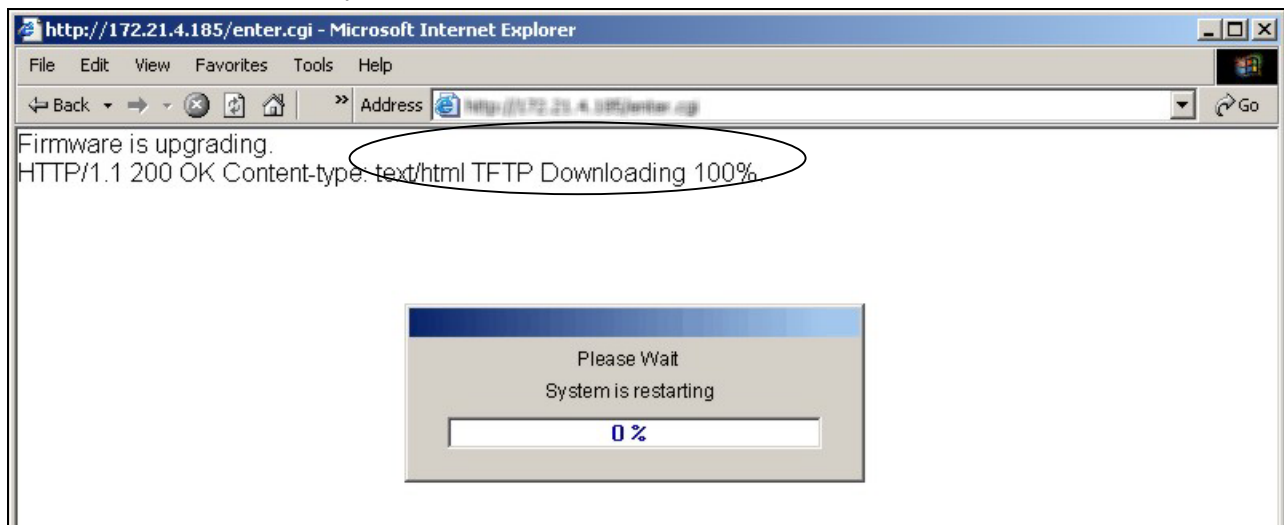
Figure 14-6 Web Configurator: Firmware Upgrade Successful

Step 7. After the VSG finishes restarting, access the web configurator again. Check the firmware version number in the login screen.

14.4 Configuration File Maintenance

You can only use the web configurator to perform configuration file backup and restore.

WARNING!
DO NOT INTERRUPT THE FILE TRANSFER PROCESS AS THIS MAY PERMANENTLY DAMAGE YOUR DEVICE.

14.4.1 Backup Configuration

Backup is highly recommended once your VSG is functioning properly.

Step 1. Run a TFTP server program on a computer and specify the location for saving the configuration file and set the communication mode.

Step 2. From the **Main Menu** screen, click **Utilities** and **Import/Export Configuration**. A screen displays as shown next.

Figure 14-7 Web Configurator: Utilities: Exporting Configuration File

Step 3.   Select **Export** and enter the IP address of the computer running the TFTP server in the **TFTP Server IP Address** field.

Step 4.   In the **Filename** field, specify the name of the configuration file to be stored and click **Apply** to start the file transfer process.

Step 5.   When the file transfer is completed successfully, the **Utilities Menu** screen displays. The configuration file should be stored in the location specified on the computer running the TFTP server.

14.4.2   Restore Configuration

This section shows you how to restore a previously saved configuration.

This function erases the current configuration before restoring a previous back up configuration; please do not attempt to restore unless you have a backup configuration file stored on disk.

Step 1.   Run a TFTP server program on a computer and specify the location for saving the configuration file and set the communication mode.

Step 2.   From the **Main Menu** screen, click **Utilities** and **Import/Export Configuration**. A screen displays as shown next.

Figure 14-8 Web Configurator: Utilities: Importing Configuration File

Step 3.   Select **Import** and enter the IP address of the computer running the TFTP server in the **TFTP Server IP Address** field.

Step 4.   In the **Filename** field, specify the name of the configuration file to import and click **Apply** to start the file transfer process.

Step 5.   When the file transfer is completed successfully, click **Restart** to reboot the VSG and make the changes take effect.

Figure 14-9 Web Configurator: Utilities: Restore Configuration: Reboot

Chapter 15
Troubleshooting

This chapter covers potential problems and possible remedies. After each problem description, some instructions are provided to help you to diagnose and to solve the problem.

15.1 Using LEDs to Diagnose Problems

The LEDs are useful aides for finding possible problem causes.

15.1.1   The Power LED

The **PWR** LED on the front panel does not light up.

Table 15-1 Troubleshooting Power LED

STEPS	CORRECTIVE ACTION
1	Check the connections from the VSG to the power source. Make sure you are using the supplied power cord and proper power supply. Refer to the product specifications.
2	Make sure the power source is turned on and that the VSG is receiving sufficient power.
3	If these steps fail to correct the problem, contact your local distributor for assistance.

15.1.2   The LAN LEDs

None of the LEDs for the LAN port light up when connected to an Ethernet device.

Table 15-2 Troubleshooting LAN LEDs

STEPS	CORRECTIVE ACTION
1	Make sure you are using the correct Ethernet cable. Connect the LAN port to a hub/switch using a crossover Ethernet cable or directly to a computer using a straight-through Ethernet cable.
2	Verify that the attached device(s) is turned on and properly connected to the VSG.
3	Verify that Ethernet cable length does not exceed 100 meters.
4	Make sure the network adapters are working on the attached devices.

15.1.3   The WAN LEDs

None of the LEDs for the WAN port light up when connected to an Ethernet device.

Table 15-3 Troubleshooting WAN LEDs

STEPS	CORRECTIVE ACTION
1	Make sure you are using the correct Ethernet cable. Connect the WAN port to a router using a straight-through Ethernet cable or directly to a computer using a crossover Ethernet cable.
2	Verify that the attached device(s) is turned on and properly connected to the VSG.
3	Verify that Ethernet cable length does not exceed 100 meters.
4	Make sure the network adapters are working on the attached devices.

15.2Console Port

I cannot access the VSG through the console port.

Table 15-4 Troubleshooting Console Port

STEPS	CORRECTIVE ACTION	
1	Check to see if the VSG is connected to your computer using a console cable.	
2	Check to see if the communications program is configured correctly. Set the communication parameters as stated here.	Emulation: auto detect Baud Rate: 9600 bps No Parity, 8 data bits, 1 stop bit Flow Control: None
3	Make sure you entered the correct username and password. The default username is "admin" and the default password is "1234". The username and password are case-sensitive. If you have forgotten your administrator username and/or password, refer to *Section 15.5*.	

15.3Web Configurator

I cannot access the web configurator.

Table 15-5 Troubleshooting Web Configurator

STEPS	CORRECTIVE ACTION
1	Make sure you are connected to the VSG on the WAN. You cannot configure the VSG on the LAN.
2	Make sure you are using the correct WAN IP address. Check the WAN IP address of the VSG in the SMT.
3	Make sure you entered the correct username and password. The default username is "admin" and the default password is "1234". The username and password are case-sensitive. If you have forgotten your administrator username and/or password, refer to *Section 15.5*.
4	Ping the VSG from your computer on the WAN. If you cannot ping the VSG, check the IP addresses of the VSG and your computer. Make sure that both IP addresses are in the same subnet.

The web configurator does not display properly.

Table 15-6 Troubleshooting Internet Browser Display

STEPS	CORRECTIVE ACTION
1	Make sure you are using either Internet Explorer (version 5.0 and later) or Netscape Navigator (version 6.0 and later).
2	Delete the temporary web files and log in again. In Internet Explorer, click **Tools**, **Internet Options** and then click the **Delete Files ...** button. When a **Delete Files** window displays, select **Delete all offline content** and click **OK**. (Steps may vary depending on the version of your Internet browser.) In Netscape, click **Edit**, **Preference**. Under **Advanced** category, click **Cache**. Click **Clear Memory Cache** and **Clear Disk Cache**. (Steps may vary depending on the version of your Internet browser.)

15.4Internet Access

A subscriber cannot connect to the Internet through the VSG.

Table 15-7 Troubleshooting Internet Access

STEPS	CORRECTIVE ACTION
1	Check the Internet settings on your modem and/or router.
2	Make sure the subscriber enter the correct user name and password to log in to the VSG. The username and password are case-sensitive.
3	Make sure the subscriber account is still valid.
4	Make sure there is no conflict in IP address assignment. Refer to the appendix.

15.5 TFTP File Transfer

I cannot perform TFTP file transfer.

Table 15-8 Troubleshooting TFTP File Transfer

STEPS	CORRECTIVE ACTION
1	Make sure the TFTP server computer is connected to the WAN port on the VSG.
2	Make sure you enter the correct TFTP server IP address and filename.
3	Make sure the IP addresses of the TFTP server and VSG are on the same subnet.
4	Check the security settings on the TFTP server. Make sure security settings do not prevent any file transfer.

15.6 Administrator Password and Username

If you have forgotten the administrator password and/username, you cannot access the VSG. You *must* reload the firmware to the VSG through the console port. Follow the steps below to reload the firmware.

Before you continue, you *must* have a firmware file.

1. Connect your computer directly to the VSG through the console port and the WAN port. Refer to the *Hardware Connections* section for more details.

2. Unplug and plug in the power cord to restart the VSG. During the system startup, enter "debug" at the "Loading … " line. Note that you will not see any characters displayed on the screen as you enter the word.
    A **Password** field should display indicating you have entered the debug mode successfully. Otherwise repeat step 3. Enter "debugmonitor" as the password. The password is case sensitive.

```
PnP GATEWAY Boot ROM Version 1.01
Ethernet Address:
  WAN : 00-a0-c5-41-d0-53
  LAN : 00-a0-c5-41-d0-49

RTC TEST OK
FLASH INIT OK
Loading...

Password:
```

Figure 15-1 SMT: Entering Debug Mode

3. Enter 3 to erase the firmware on the VSG.

```
(1)Run Monitor
(2)Restart system
(3)Erase entire FLASH
(4)SDRAM Testing
Enter selection:3
Erasing flash 0 block 0...OK
Erasing flash 0 block 1...OK
Erasing flash 0 block 2...OK
Erasing flash 0 block 3...OK
Erasing flash 0 block 4...OK


…

Erasing flash 0 block 16...OK
Erasing flash 0 block 17...OK
Erasing flash 0 block 18...OK
Erasing flash 0 block 19...OK
Erasing flash 0 block 20...OK
Erasing flash 0 block 21...OK
Erasing flash 0 block 22...OK
```

Figure 15-2 SMT: Debug Mode: Erasing Firmware

4. Enter 2 to restart the VSG.

```
(1)Run Monitor
(2)Restart system
(3)Erase entire FLASH
(4)SDRAM Testing
Enter selection:2

Restarting...
```

Figure 15-3 SMT: Debug Mode: Restarting the VSG

5. After the VSG restarts, a screen displays prompting you to specify the initial settings for TFTP file transfer. The default settings are displayed in the brackets.
For VSG settings, specify the IP address, subnet mask and default gateway. For TFTP server settings, enter the IP address and the firmware file name.

Make sure the IP addresses are in the same range.

```
-------------------------------------------------
Please enter TFTP related parameters:

IP address[192.168.1.254]:10.59.1.1
TFTP server IP address[192.168.1.253]:10.59.1.33
Gateway IP address[192.168.1.1]:10.59.1.33
Subnet mask[255.255.255.0]:255.0.0.0
File name[IBOX.BIN]:VSG1000-10303.bin
```

Figure 15-4 SMT: Debug Mode: Specifying Initial VSG and TFTP Settings

6. Verify the settings and enter **n**. Otherwise enter **y** to change the settings again.

```
----------- TFTP download parameters -----------

  IP address             :10.59.1.1
  TFTP server IP address :10.59.1.33
  Gateway IP address     :10.59.1.33
  Subnet mask            :255.0.0.0
  File name              :VSG1000-10303.bin


-----------------------------------------------

Do you want to change above entries(Y/N)?n
```

Figure 15-5 SMT: Debug Mode: Verifying VSG and TFTP Settings

7. The VSG downloads the firmware. After the file transfer is complete, the VSG restarts automatically.

```
Do you want to change above entries(Y/N)?n
Attached TCP/IP interface to rtl1.
Attaching network interface lo0... done.

Downloading...

100%

Erasing FLASH...OK
Writing to FLASH...OK
Restarting...
```

Figure 15-6 SMT: Debug Mode: Firmware Upload Complete

8. After the VSG finishes restarting, you should see the "Press any key to continue" prompt, press any key to display the SMT login screen. Enter "admin" as the username and "1234" as the password to access the VSG.

Appendix A
IP Address Assignment Conflicts

This appendix describes situations where IP address conflicts may occur. Subscribers with duplicate IP addresses will not be able to access the Internet.

Case A: The VSG is using the same LAN and WAN IP addresses

The following figure shows an example where the VSG is using a WAN IP address that is the same as the IP address of a computer on the LAN.
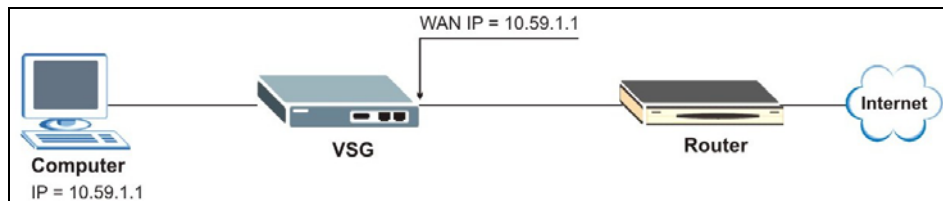
Diagram 1 IP Address Conflicts: Case A

You must set the VSG to use different LAN and WAN IP addresses on different subnets if you enable DHCP server on the VSG. For example, you set the WAN IP address to 192.59.1.1 and the LAN IP address to 10.59.1.1. Otherwise, It is recommended the VSG use a public WAN IP address.

Case B: The VSG LAN IP address conflicts with the DHCP client IP address

In the following figure, the VSG is acting as a DHCP server. The VSG assigns an IP address, which is the same as its LAN port IP address, to a DHCP client attached to the LAN.
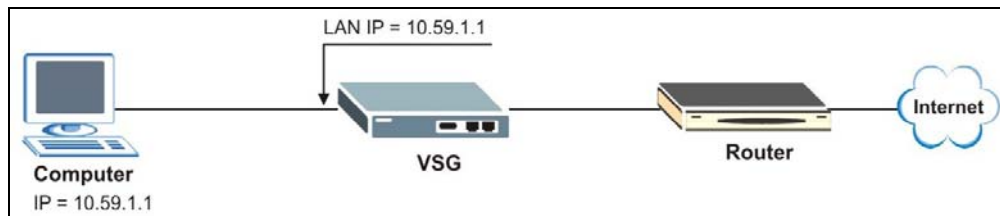
Diagram 2 IP Address Conflicts: Case B

To solve this problem, make sure the VSG LAN IP address is not in the DHCP IP address pool.

Case C: The Subscriber IP address is the same as the IP address of a network device

The following figure depicts an example where the subscriber IP address is the same as the IP address of a network device not attached to the VSG.
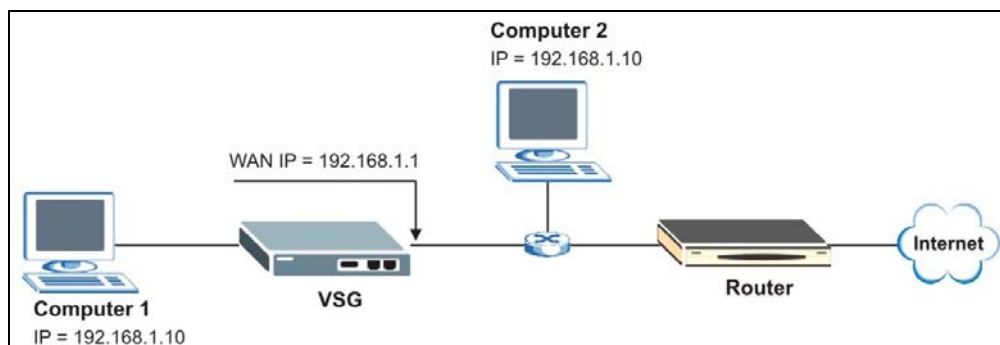
Diagram 3 IP Address Conflicts: Case C

You must set the VSG to use different LAN and WAN IP addresses on different subnets if you enable DHCP server on the VSG. For example, you set the WAN IP address to 192.59.1.1 and the LAN IP address to 10.59.1.1. Otherwise, It is recommended the VSG use a public WAN IP address.

Case D: Two or more subscribers have the same IP address.

By converting all private IP addresses to the WAN IP address, the VSG allows subscribers with different network configurations to access the Internet. However, there are situations where two or more subscribers are using the same private IP address. This may happen when a subscriber is configured to use a static (or fixed) IP address that is the same as the IP address the VSG DHCP server assigns to another subscriber acting as a DHCP client.

In this case, the subscribers are not able to access the Internet.
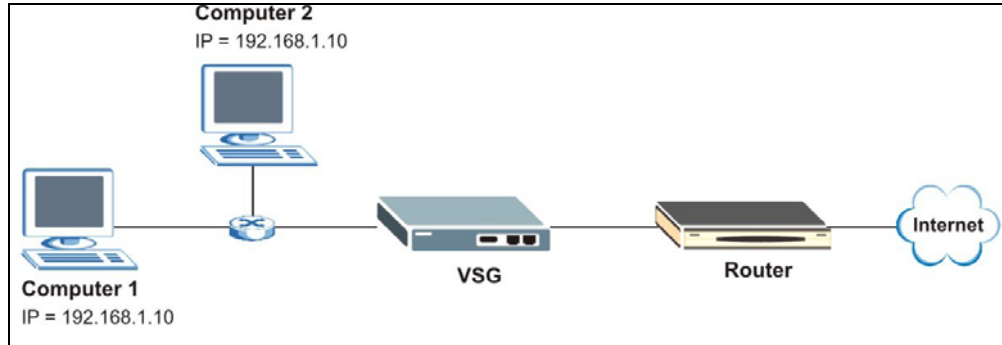
Diagram 4 IP Address Conflicts: Case D

This problem can be solved by adding a VLAN-enabled switch or set the computers to obtain IP addresses dynamically.

Appendix B
Subscriber Login

To log in as a subscriber, enter a web site address such as www.zyxel.com in a web browser.

The login screen displays prompting you to enter the user name and password.
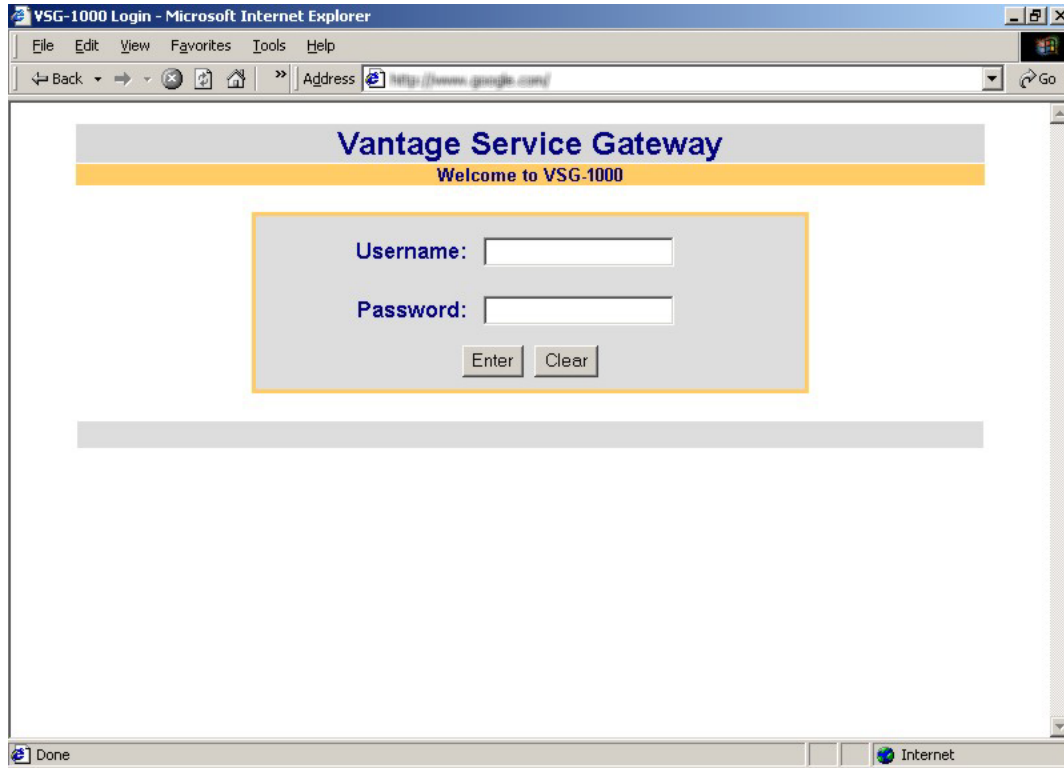
Diagram 5 Subscriber Login Screen

Enter a user name and password and click **Enter**. Depending on the settings in the VSG, either the specified web page or an advertisement web page displays. A logout window may also display.

Appendix C
Cable Types and Cable Pin Assignments

RJ-45 Ethernet Port

The following table describes the types of network cable used for the different connection speeds.

Make sure the Ethernet cable length between connections does not exceed 100 meters (328 feet).
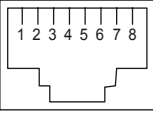
Chart A Network Cable Types

SPEED	NETWORK CABLE TYPE
10 Base-TX	100Ω 2-pair UTP/STP Category 3, 4 or 5
100 Base-TX	100Ω 2-pair UTP/STP Category 5

The WAN Port

The following table describes the Ethernet cable pin assignment for the WAN port.

Chart B WAN Port Cable Ping Assignments

PIN NO	RJ-45 SIGNAL ASSIGNMENT	DESIGNATION
1	Output Transmit Data +	TD+
2	Output Transmit Data -	TD-
3	Input Transmit Data +	RD+
4	Unused	N/U
5	Unused	N/U
6	Input Transmit Data -	RD-
7	Unused	N/U
8	Unused	N/U

Make sure that the Ethernet cable connection between the VSG and the hub or router conforms to the pin assignments as shown in the following diagram.
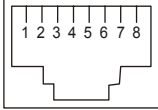
ETHERNET DEVICE (SWITCH/HUB/ROUTER ETC.)		VANTAGE SERVICE GATEWAY	
1	RD+	1	TD+
2	RD-	2	TD-
3	TD+	3	RD+
6	TD-	6	RD-

Diagram 6 WAN Port Cable Pin Assignments

The LAN Port

The following table describes the Ethernet cable pin assignment for the LAN port.

Chart C LAN Port Cable Pin Assignments

	PIN NO	RJ-45 SIGNAL ASSIGNMENT	DESIGNATION
	1	Input Transmit Data +	RD+
	2	Input Transmit Data -	RD-
	3	Output Transmit Data +	TD+
1 2 3 4 5 6 7 8	4	Unused	N/U
	5	Unused	N/U
	6	Output Transmit Data -	TD-
	7	Unused	N/U
	8	Unused	N/U

Make sure that the Ethernet cable connection between the VSG and a computer or switch uplink port conforms to the pin assignments as shown in the figure.
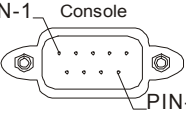
ETHERNET DEVICE (COMPUTER/ UPLINK PORT)			VANTAGE SERVICE GATEWAY	
1	TD+		1	RD+
2	TD-		2	RD-
3	RD+		3	TD+
6	RD-		6	TD-

Diagram 7 LAN Port Cable Pin Assignments

Serial Console Port

The following table describes the console cable pin assignment for the serial console port.

Chart D Console Port Pin Assignment

	PIN NO	MNEMONIC	FUNCTION
	1	DCD	Received Line Signal Detector to the VSG.
PIN-1 Console	2	TXT	Transmitted Data from the VSG.
	3	RXT	Received Data to the VSG.
	4	DTR	Data Terminal Ready from the VSG.
PIN-9	5	GND	Signal Ground (Common)
	6	DSR	Data Set Ready to the VSG.
	7	RTS	Request to Send from the VSG.
	8	CTS	Clear to Send to the VSG.
	9	RI	Ring Indicator to the VSG.

Appendix D
Setting Your Computer IP Address

All computers must have a 10M or 100M Ethernet adapter and TCP/IP installed.

Windows 95/98/Me/NT/2000/XP, Macintosh OS 7 and later operating systems and all versions of UNIX/LINUX include the software components you need to install and use TCP/IP on your computer. Windows 3.1 requires the purchase of a third-party TCP/IP application package.

TCP/IP should already be installed on computers using Windows NT/2000/XP, Macintosh OS 7 and later operating systems.

After the appropriate TCP/IP components are installed, configure the TCP/IP settings in order to "communicate" with your network.

If you manually assign IP information instead of using dynamic assignment, make sure that your computers have IP addresses that place them in the same subnet as the VSG's LAN port (for Internet access) or WAN port (for remote management).

Windows 95/98/Me

Click **Start**, **Settings**, **Control Panel** and double-click the **Network** icon to open the **Network** window.
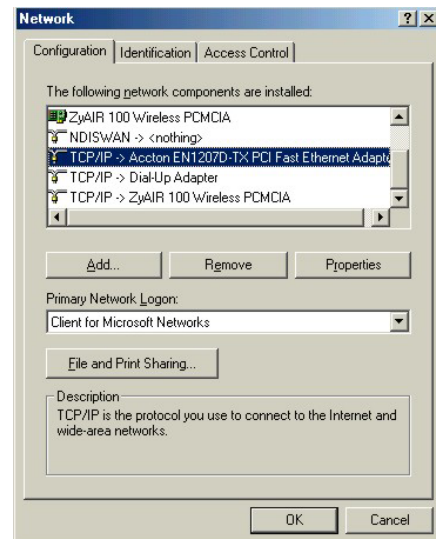
Installing Components

The **Network** window **Configuration** tab displays a list of installed components. You need a network adapter, the TCP/IP protocol and Client for Microsoft Networks.

If you need the adapter:

a.   In the **Network** window, click **Add**.

b.   Select **Adapter** and then click **Add**.

c.   Select the manufacturer and model of your network adapter and then click **OK**.

If you need TCP/IP:

a.   In the **Network** window, click **Add**.

b.   Select **Protocol** and then click **Add**.

c.   Select **Microsoft** from the list of **manufacturers**.

d.   Select **TCP/IP** from the list of network protocols and then click **OK**.

If you need Client for Microsoft Networks:

a. Click **Add**.

b. Select **Client** and then click **Add**.

c. Select **Microsoft** from the list of manufacturers.

d. Select **Client for Microsoft Networks** from the list of network clients and then click **OK**.

e. Restart your computer so the changes you made take effect.

Configuring

1. In the **Network** window **Configuration** tab, select your network adapter's TCP/IP entry and click **Properties**.

2. Click the **IP Address** tab.

    -If your IP address is dynamic, select **Obtain an IP address automatically**.

    -If you have a static IP address, select **Specify an IP address** and type your information into the **IP Address** and **Subnet Mask** fields.
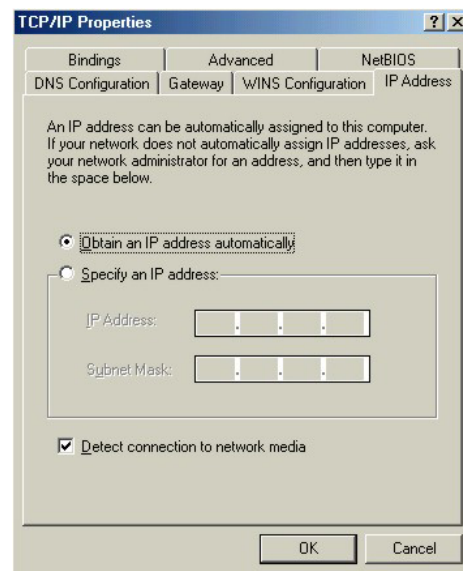
3. Click the **DNS** Configuration tab.

    -If you do not know your DNS information, select **Disable DNS**.

    -If you know your DNS information, select **Enable DNS** and type the information in the fields below (you may not need to fill them all in).
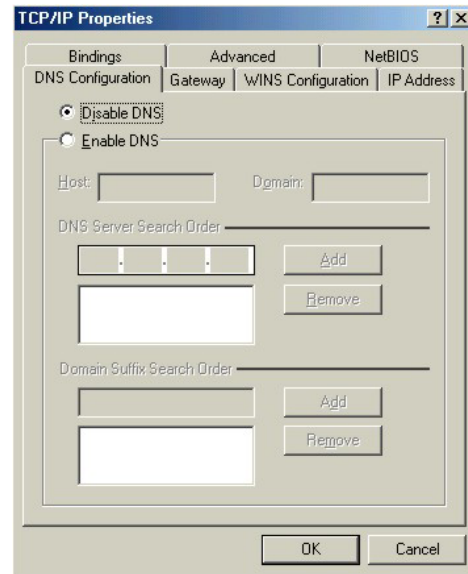
4. Click the **Gateway** tab.

    -If you do not know your gateway's IP address, remove previously installed gateways.

    -If you have a gateway IP address, type it in the **New gateway field** and click **Add**.
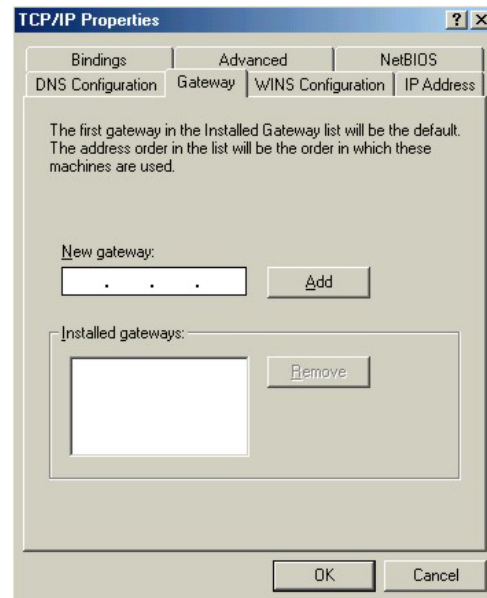
5. Click **OK** to save and close the **TCP/IP Properties** window.

6. Click **OK** to close the **Network** window. Insert the Windows CD if prompted.

7. Turn on your VSG and restart your computer when prompted.

Verifying Settings

1. Click **Start** and then **Run**.

2. In the **Run** window, type "winipcfg" and then click **OK** to open the **IP Configuration** window.

3. Select your network adapter. You should see your computer's IP address, subnet mask and default

gateway.

Windows 2000/NT/XP

1. For Windows XP, click **start**, **Control Panel**. In Windows 2000/NT, click **Start**, **Settings**, **Control Panel**.
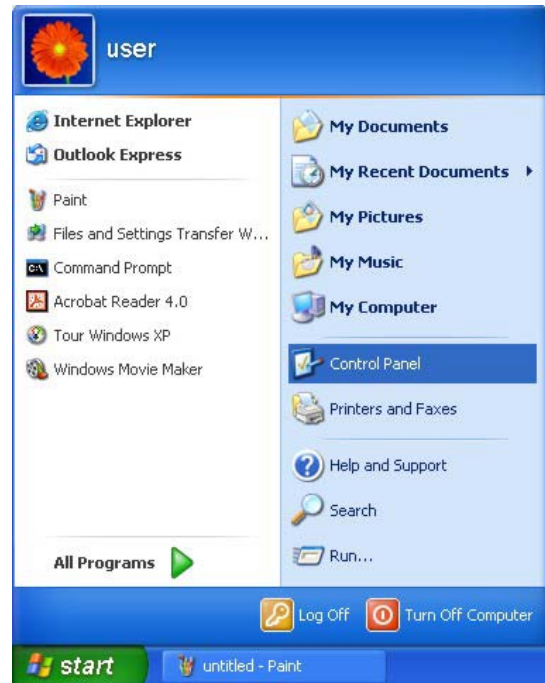
2. For Windows XP, click **Network Connections**. For Windows 2000/NT, click **Network and Dial-up Connections**.

3. Right-click **Local Area Connection** and then click **Properties**.
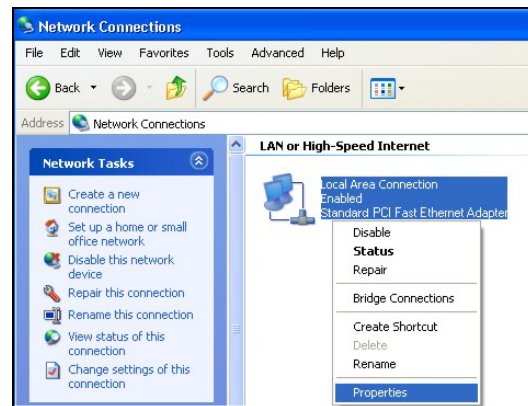
4. Select **Internet Protocol (TCP/IP)** (under the **General** tab in Win XP) and click **Properties**.
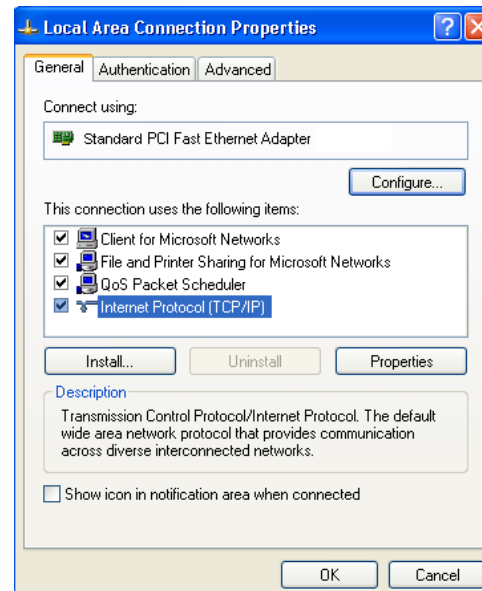
5. The **Internet Protocol TCP/IP Properties** window opens (the **General tab** in Windows XP).

   -If you have a dynamic IP address click **Obtain an IP address automatically**.

   -If you have a static IP address click **Use the following IP Address** and fill in the **IP address**, **Subnet mask**, and **Default gateway** fields.

   Click **Advanced**.
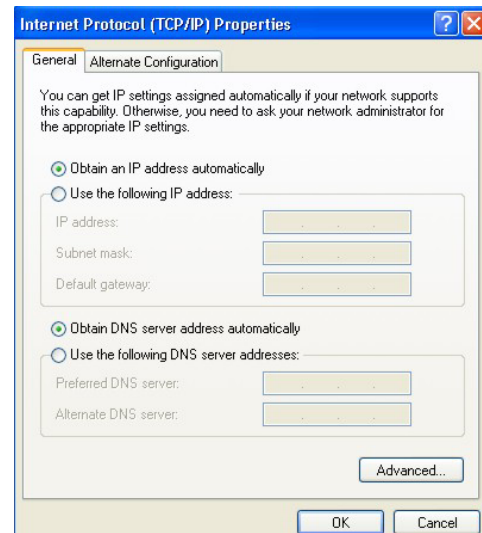
6. -If you do not know your gateway's IP address, remove any previously installed gateways in the **IP Settin**gs tab and click **OK**.

    Do one or more of the following if you want to configure additional IP addresses:

    -In the **IP Settings** tab, in IP addresses, click **Add**.

    -In **TCP/IP Address**, type an IP address in **IP address** and a subnet mask in **Subnet mask**, and then click **Add**.

    -Repeat the above two steps for each IP address you want to add.

    -Configure additional default gateways in the **IP Settings** tab by clicking **Add** in **Default gateways**.

    -In **TCP/IP Gateway Address**, type the IP address of the default gateway in **Gateway**. To manually configure a default metric (the number of transmission hops), clear the **Automatic metric** check box and type a metric in **Metric**.

    -Click **Add**.

    -Repeat the previous three steps for each default gateway you want to add.

    -Click **OK** when finished.
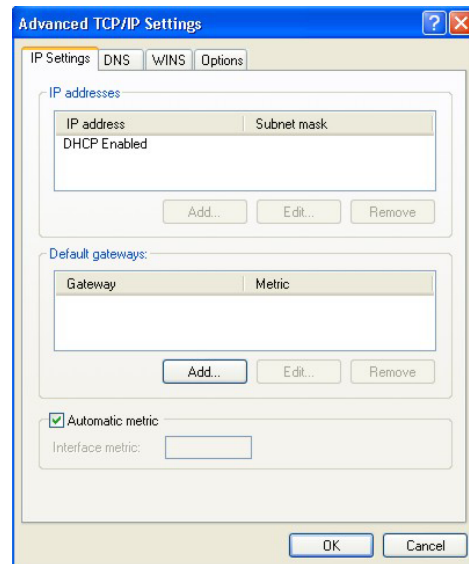
7. In the **Internet Protocol TCP/IP Properties** window (the **General tab** in Windows XP):

    -Click **Obtain DNS server address automatically** if you do not know your DNS server IP address(es).

    -If you know your DNS server IP address(es), click **Use the following DNS server addresses**, and type them in the **Preferred DNS server** and **Alternate DNS server** fields.

    If you have previously configured DNS servers, click **Advanced** and then the **DNS** tab to order them.
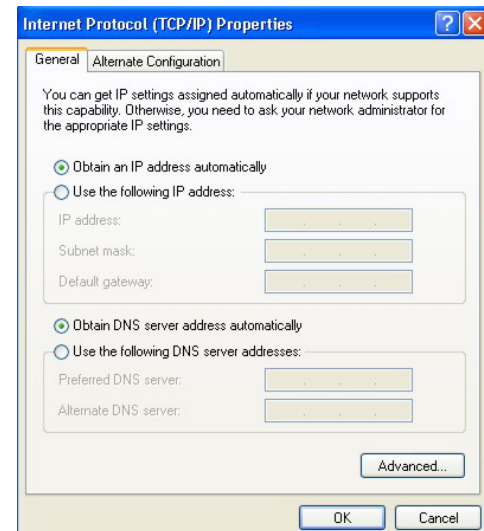
8. Click **OK** to close the **Internet Protocol (TCP/IP) Properties** window.

9. Click **OK** to close the **Local Area Connection Properties** window.

10. Turn on your VSG and restart your computer (if prompted).

Verifying Settings

1. Click **Start**, **All Programs**, **Accessories** and then **Command Prompt**.

2. In the **Command Prompt** window, type "ipconfig" and then press [ENTER]. You can also open **Network Connections**, right-click a network connection, click **Status** and then click the **Support** tab.

Macintosh OS 8/9

1. Click the **Apple** menu, **Control Panel** and double-click **TCP/IP** to open the **TCP/IP Control Panel**.

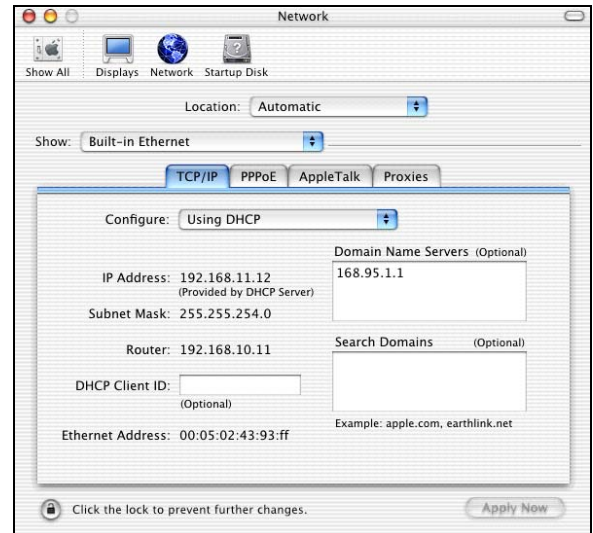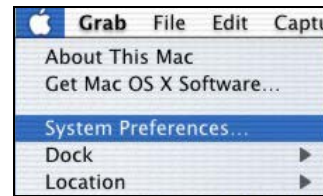2. Select **Ethernet built-in** from the **Connect via** list.
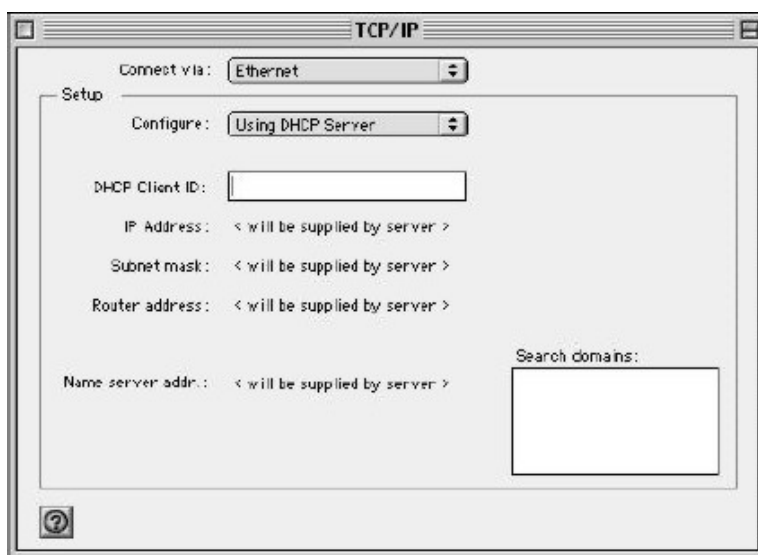
3. For dynamically assigned settings, select **Using DHCP Server** from the **Configure:** list.

4. For statically assigned settings, do the following:

    -From the **Configure** box, select **Manually**.

    -Type your IP address in the **IP Address** box.

    -Type your subnet mask in the **Subnet mask** box.

    -Type the IP address of your VSG in the **Router address** box.

5. Close the **TCP/IP Control Panel**.

6. Click **Save** if prompted, to save changes to your configuration.

7. Turn on your VSG and restart your computer (if prompted).

Verifying Settings

Check your TCP/IP properties in the **TCP/IP Control Panel** window.

Macintosh OS X

1. Click the **Apple** menu, and click **System Preferences** to open the **System Preferences** window.

2. Click **Network** in the icon bar.
   - Select **Automatic** from the **Location** list.
   - Select **Built-in Ethernet** from the **Show** list.
   - Click the **TCP/IP** tab.

3. For dynamically assigned settings, select **Using DHCP** from the **Configure** list.

4. For statically assigned settings, do the following:

   -From the **Configure** box, select **Manually**.

   -Type your IP address in the **IP Address** box.

   -Type your subnet mask in the **Subnet mask** box.

   -Type the IP address of your VSG in the **Router address** box.

5. Click **Apply Now** and close the window.

6. Turn on your VSG and restart your computer (if prompted).

Verifying Settings

Check your TCP/IP properties in the **Network** window.

Appendix E
IP Subnetting

IP Addressing

Routers "route" based on the network number. The router that delivers the data packet to the correct destination host uses the host ID.

IP Classes

An IP address is made up of four octets (eight bits), written in dotted decimal notation, for example, 192.168.1.1. IP addresses are categorized into different classes. The class of an address depends on the value of its first octet.

➢ Class "A" addresses have a 0 in the left most bit. In a class "A" address the first octet is the network number and the remaining three octets make up the host ID.

➢ Class "B" addresses have a 1 in the left most bit and a 0 in the next left most bit. In a class "B" address the first two octets make up the network number and the two remaining octets make up the host ID.

➢ Class "C" addresses begin (starting from the left) with 1 1 0. In a class "C" address the first three octets make up the network number and the last octet is the host ID.

➢ Class "D" addresses begin with 1 1 1 0. Class "D" addresses are used for multicasting. (There is also a class "E" address. It is reserved for future use.)

Chart 5 Classes of IP Addresses

IP ADDRESS:		OCTET 1	OCTET 2	OCTET 3	OCTET 4
Class A	0	Network number	Host ID	Host ID	Host ID
Class B	10	Network number	Network number	Host ID	Host ID
Class C	110	Network number	Network number	Network number	Host ID

Host IDs of all zeros or all ones are not allowed.

Therefore:

➢ A class "C" network (8 host bits) can have $2^8 - 2$ or 254 hosts.

➢ A class "B" address (16 host bits) can have $2^{16} - 2$ or 65534 hosts.

A class "A" address (24 host bits) can have $2^{24} - 2$ hosts (approximately 16 million hosts).

Since the first octet of a class "A" IP address must contain a "0", the first octet of a class "A" address can have a value of 0 to 127.

Similarly the first octet of a class "B" must begin with "10", therefore the first octet of a class "B" address has a valid range of 128 to 191. The first octet of a class "C" address begins with "110", and therefore has a range of 192 to 223.

Chart 6 Allowed IP Address Range By Class

CLASS	ALLOWED RANGE OF FIRST OCTET (BINARY)	ALLOWED RANGE OF FIRST OCTET (DECIMAL)
Class A	**0**0000000 to **0**1111111	0 to 127
Class B	**10**000000 to **10**111111	128 to 191
Class C	**110**00000 to **110**11111	192 to 223
Class D	**1110**0000 to **1110**1111	224 to 239

Subnet Masks

A subnet mask is used to determine which bits are part of the network number, and which bits are part of the host ID (using a logical AND operation). A subnet mask has 32 bits; each bit of the mask corresponds to a bit of the IP address. If a bit in the subnet mask is a "1" then the corresponding bit in the IP address is part of the network number. If a bit in the subnet mask is "0" then the corresponding bit in the IP address is part of the host ID.

Subnet masks are expressed in dotted decimal notation just as IP addresses are. The "natural" masks for class A, B and C IP addresses are as follows.

Chart 7 "Natural" Masks

CLASS	NATURAL MASK
A	255.0.0.0
B	255.255.0.0
C	255.255.255.0

Subnetting

With subnetting, the class arrangement of an IP address is ignored. For example, a class C address no longer has to have 24 bits of network number and 8 bits of host ID. With subnetting, some of the host ID bits are converted into network number bits. By convention, subnet masks always consist of a continuous sequence of ones beginning from the left most bit of the mask, followed by a continuous sequence of zeros, for a total number of 32 bits.

Since the mask is always a continuous number of ones beginning from the left, followed by a continuous number of zeros for the remainder of the 32 bit mask, you can simply specify the number of ones instead of writing the value of each octet. This is usually specified by writing a "/" followed by the number of bits in the mask after the address.

For example, 192.1.1.0 /25 is equivalent to saying 192.1.1.0 with mask 255.255.255.128.

The following table shows all possible subnet masks for a class "C" address using both notations.

Chart 8 Alternative Subnet Mask Notation

SUBNET MASK IP ADDRESS	SUBNET MASK "1" BITS	LAST OCTET BIT VALUE
255.255.255.0	/24	0000 0000
255.255.255.128	/25	1000 0000
255.255.255.192	/26	1100 0000
255.255.255.224	/27	1110 0000
255.255.255.240	/28	1111 0000
255.255.255.248	/29	1111 1000
255.255.255.252	/30	1111 1100

The first mask shown is the class "C" natural mask. Normally if no mask is specified it is understood that the natural mask is being used.

Example: Two Subnets

As an example, you have a class "C" address 192.168.1.0 with subnet mask of 255.255.255.0.

	NETWORK NUMBER	HOST ID
IP Address	192.168.1.	0
IP Address (Binary)	11000000.10101000.00000001.	00000000
Subnet Mask	255.255.255.	0
Subnet Mask (Binary)	11111111.11111111.11111111.	00000000

The first three octets of the address make up the network number (class "C"). You want to have two separate networks.

Divide the network 192.168.1.0 into two separate subnets by converting one of the host ID bits of the IP address to a network number bit. The "borrowed" host ID bit can be either "0" or "1" thus giving two subnets; 192.168.1.0 with mask 255.255.255.128 and 192.168.1.128 with mask 255.255.255.128.

In the following charts, shaded/bolded last octet bit values indicate host ID bits "borrowed" to form network ID bits. The number of "borrowed" host ID bits determines the number of subnets you can have. The remaining number of host ID bits (after "borrowing") determines the number of hosts you can have on each subnet.

Chart 9 Subnet 1

	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	0
IP Address (Binary)	11000000.10101000.00000001.	**0**0000000
Subnet Mask	255.255.255.	128
Subnet Mask (Binary)	11111111.11111111.11111111.	**1**0000000
Subnet Address: 192.168.1.0		Lowest Host ID: 192.168.1.1
Broadcast Address: 192.168.1.127		Highest Host ID: 192.168.1.126

Chart 10 Subnet 2

	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	128
IP Address (Binary)	11000000.10101000.00000001.	**1**0000000
Subnet Mask	255.255.255.	128
Subnet Mask (Binary)	11111111.11111111.11111111.	**1**0000000
Subnet Address: 192.168.1.128		Lowest Host ID: 192.168.1.129
Broadcast Address: 192.168.1.255		Highest Host ID: 192.168.1.254

The remaining 7 bits determine the number of hosts each subnet can have. Host IDs of all zeros represent the subnet itself and host IDs of all ones are the broadcast address for that subnet, so the actual number of hosts available on each subnet in the example above is $2^7 - 2$ or 126 hosts for each subnet.

192.168.1.0 with mask 255.255.255.128 is the subnet itself, and 192.168.1.127 with mask 255.255.255.128 is the directed broadcast address for the first subnet. Therefore, the lowest IP address that can be assigned to an actual host for the first subnet is 192.168.1.1 and the highest is 192.168.1.126. Similarly the host ID range for the second subnet is 192.168.1.129 to 192.168.1.254.

Example: Four Subnets

The above example illustrated using a 25-bit subnet mask to divide a class "C" address space into two subnets. Similarly to divide a class "C" address into four subnets, you need to "borrow" two host ID bits to give four possible combinations of 00, 01, 10 and 11. The subnet mask is 26 bits (11111111.11111111.11111111.**11**000000) or 255.255.255.192. Each subnet contains 6 host ID bits, giving 2^6-2 or 62 hosts for each subnet (all 0's is the subnet itself, all 1's is the broadcast address on the subnet).

Chart 11 Subnet 1

	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	0

Chart 11 Subnet 1

	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address (Binary)	11000000.10101000.00000001.	**00**000000
Subnet Mask (Binary)	11111111.11111111.11111111.	**11**000000
Subnet Address: 192.168.1.0		Lowest Host ID: 192.168.1.1
Broadcast Address: 192.168.1.63		Highest Host ID: 192.168.1.62

Chart 12 Subnet 2

	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	64
IP Address (Binary)	11000000.10101000.00000001.	**01**000000
Subnet Mask (Binary)	11111111.11111111.11111111.	**11**000000
Subnet Address: 192.168.1.64		Lowest Host ID: 192.168.1.65
Broadcast Address: 192.168.1.127		Highest Host ID: 192.168.1.126

Chart 13 Subnet 3

	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	128
IP Address (Binary)	11000000.10101000.00000001.	**10**000000
Subnet Mask (Binary)	11111111.11111111.11111111.	**11**000000
Subnet Address: 192.168.1.128		Lowest Host ID: 192.168.1.129
Broadcast Address: 192.168.1.191		Highest Host ID: 192.168.1.190

Chart 14 Subnet 4

	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	192
IP Address (Binary)	11000000.10101000.00000001.	**11**000000
Subnet Mask (Binary)	11111111.11111111.11111111.	**11**000000
Subnet Address: 192.168.1.192		Lowest Host ID: 192.168.1.193
Broadcast Address: 192.168.1.255		Highest Host ID: 192.168.1.254

Example Eight Subnets

Similarly use a 27-bit mask to create 8 subnets (001, 010, 011, 100, 101, 110).

The following table shows class C IP address last octet values for each subnet.

Chart 15 Eight Subnets

SUBNET	SUBNET ADDRESS	FIRST ADDRESS	LAST ADDRESS	BROADCAST ADDRESS
1	0	1	30	31
2	32	33	62	63
3	64	65	94	95

Chart 15 Eight Subnets

SUBNET	SUBNET ADDRESS	FIRST ADDRESS	LAST ADDRESS	BROADCAST ADDRESS
4	96	97	126	127
5	128	129	158	159
6	160	161	190	191
7	192	193	222	223
8	224	223	254	255

The following table is a summary for class "C" subnet planning.

Chart 16 Class C Subnet Planning

NO. "BORROWED" HOST BITS	SUBNET MASK	NO. SUBNETS	NO. HOSTS PER SUBNET
1	255.255.255.128 (/25)	2	126
2	255.255.255.192 (/26)	4	62
3	255.255.255.224 (/27)	8	30
4	255.255.255.240 (/28)	16	14
5	255.255.255.248 (/29)	32	6
6	255.255.255.252 (/30)	64	2
7	255.255.255.254 (/31)	128	1

Subnetting With Class A and Class B Networks.

For class "A" and class "B" addresses the subnet mask also determines which bits are part of the network number and which are part of the host ID.

A class "B" address has two host ID octets available for subnetting and a class "A" address has three host ID octets (see *Chart 5*) available for subnetting.

The following table is a summary for class "B" subnet planning.

Chart 17 Class B Subnet Planning

NO. "BORROWED" HOST BITS	SUBNET MASK	NO. SUBNETS	NO. HOSTS PER SUBNET
1	255.255.128.0 (/17)	2	32766
2	255.255.192.0 (/18)	4	16382
3	255.255.224.0 (/19)	8	8190
4	255.255.240.0 (/20)	16	4094
5	255.255.248.0 (/21)	32	2046
6	255.255.252.0 (/22)	64	1022
7	255.255.254.0 (/23)	128	510
8	255.255.255.0 (/24)	256	254
9	255.255.255.128 (/25)	512	126
10	255.255.255.192 (/26)	1024	62
11	255.255.255.224 (/27)	2048	30

Chart 17 Class B Subnet Planning

NO. "BORROWED" HOST BITS	SUBNET MASK	NO. SUBNETS	NO. HOSTS PER SUBNET
12	255.255.255.240 (/28)	4096	14
13	255.255.255.248 (/29)	8192	6
14	255.255.255.252 (/30)	16384	2
15	255.255.255.254 (/31)	32768	1

Appendix F
Product Specifications

GENERAL	
Standard	IEEE 802.3 10BASE-T Ethernet
	IEEE 802.3u 100BASE-TX Fast Ethernet
Interface	One 10/100 Ethernet WAN port
	One 10/100 Ethernet LAN port
	One RS232 console port
Networking	Plug-and-play subscriber Internet access
	NAT (RFC1631)
	NAT for VPN (IPSec/PPTP)
	DHCP server and DHCP relay
	HTTP proxy
	SMTP redirection
	WAN connection (static IP/ DHCP client)
AAA	Web-based authentication
	RADIUS AAA
	Secondary RADIUS server
	Global roaming support
	Built-in authentication and accounting
	Proprietary CAS (Central Authentication Service)
Security	L2 isolation
	VPN pass through (IPSec/ PPTP/ L2TP)
	IP/MAC address pass through
Other	Walled garden
	Advertisement URL link
	Home page re-direction
	Customized subscriber login page

PERFORMANCE & MANAGEMENT	
Max. Throughput*	15.2Mbps
Concurrent User	1,024
Management	Web-based management
	TFTP firmware upgrade
	Remote authorized management
	Configuration file import/export
	LAN device management

PHYSICAL & ENVIRONMENT	
LED	Power
	WAN: 10, 100, LK/ACT
	LAN: 10,100, LK/ACT

PHYSICAL & ENVIRONMENT	
Dimension	440(W) x 116(L) x 44(H) mm
Temperature	0 to 50C
Humidity	10% to 95% (non-condensing)
Power	100-220 V AC, 50/60 Hz Maximum power consumption: 20W
Certification	FCC part 15 Class A VCCI Class A UL Class A CE

Index

H

I

L

M

N

O

P

R

S

T

U

V

W

Z